序

编写本书有双重的目的．前十章可以作为群论课程的基础，因而每章末尾都有习题．后十章可以用作选修课材料或参考资料．本书用作课本时，要求学生具有近世代数入门课程的知识，即相当于勃霍夫和麦克兰的《近世代数概论》(Birkhoff and MacLane [1]) 的内容[1]．我尽可能使本书是独立的，凡是需要预备知识的地方，都给出了参考文献，主要是勃霍夫和麦克兰的书．

当代群论方面的研究是活跃的和广泛的，这可以从《数学评论》(Mathematical Reviews) 上刊载的文章来证实．要想概括全部主题或列举完全的文献，是不太可能的．因此我在很大程度上根据自己的兴趣来选择讨论的主题，参考文献也只限于列出本书所参考的．某些很重要课题的详细研究在新近的出版物中是很容易找到的，所以对于这些课题的论述我就力求精简．关于无限阿贝尔群的详细讨论，读者可以参考库罗什的《群论》[Kurosch (Курош)[2]][2] 和卡泼伦斯基的专著《无限阿贝尔群》(Kaplansky[1]) 的适当部分．同属于爱尔格勃尼色丛书 (Ergebnisse series) 的铃木通夫的《群的结构及其子群的格的结构》(Suzuki[1]) 及柯克色特和摩色尔的《离散群的生成元素和关系》(Coxeter and Moser, Generators

---

1) 学过高等代数的读者，只要再具有张禾瑞著《近世代数》一书的知识．——译者

2) 有中译本：А. Г. 库罗什，群论，人民教育出版社，1964．——译者

and Relations for Discrete Groups)[1]，可以供希望进一步研究这些课题的读者参考.

本书是从我在俄亥俄州立大学多年的群论课程的讲稿发展而成的. 本书的主要部分是 1956 年在剑桥的三一学院写的。（下略）

M. 赫　尔
于俄亥俄州哥伦布城

1）这本书未列在书末文献中. ——译者

目　　录

第一章 引 论

1.1. 代数定律

代数学有很大一部分是探讨元素的体系的，这些元素象数一样，可以用加法或乘法或同时用两者把它们结合起来．设给定一个由字母 $a, b, c, \cdots$ 表示的元素的体系．我们把这个体系记做 $S = S(a, b, c, \cdots)$．这种体系的性质取决于下列基本定律中有哪一些成立：

闭合律　　$A0$. 加法有意义．　　$M0$. 乘法有意义．

这就是说，对于 S 的每一对有序的元素 a 和 b，$a + b = c$ 存在而且是 S 的唯一的元素，又 $ab = d$ 也存在而且是 S 的唯一的元素．

结合律　　$A1$. $(a + b) + c = a + (b + c)$．　　$M1$. $(ab)c = a(bc)$．

交换律　　$A2$. $b + a = a + b$．　　$M2$. $ba = ab$．

零和单位元素　$A3$. 0 存在，使得对于所有的 a 都有 $0 + a = a + 0 = a$．　　$M3$. 1 存在，使得对于所有的 a 都有 $1a = a1 = a$．

负和逆　　$A4$. 对于每个　　$M4$.[1] 对于每个

1）这里提出的 $M4$ 的表述适用于加法和乘法都有意义的体系． 如果加法没有意义，因而在 S 内没有 0，那么这定律可以改写成："对于每个 a，a^{-1} 存在，使得 $(a^{-1})a = a(a^{-1}) = 1$．"

	a, $-a$存在，使得 $(-a)+a=a+(-a)=0$.	$a\neq 0$, a^{-1}存在，使得 $(a^{-1})a=a(a^{-1})=1$.
分配律	D1. $a(b+c)=ab+ac$.	
	D2. $(b+c)a=ba+ca$.	

定义．满足所有这些定律的体系叫做域．满足 $A0$, $A1$, $A2$, $A3$, $A4$, $M0$, $M1$ 和 $D1$, $D2$ 的体系叫做环．

值得指出，除去在 $M4$ 中 0 的逆不存在以外，$A0$-$A4$ 和 $M0$-$M4$ 是完全平行的．然而在分配律中，加法和乘法是绝然不同的．加法和乘法之间的这种平行性可以用对数来说明．在对数理论里，加法和乘法之间的基本的对应关系是以下的公式：

$$\log(xy)=\log x+\log y.$$

一般地说，集合 S 的一个 n 元运算是以 S 的元素 $a_1,\cdots,a_n$ 为元的 n 元函数 $f=f(a_1,\cdots,a_n)$，当 f 对于这些元有定义时，它的值 $f(a_1,\cdots,a_n)=b$ 是 S 的唯一的元素．如果对于在 S 中任意选取的 $a_1,\cdots,a_n$, $f(a_1,\cdots,a_n)$ 都有定义，我们就说运算 f 在 S 上有意义或者说集合 S 对于运算 f 来说是闭合的．

在域 F 内，加法和乘法都是有意义的二元运算，而逆运算 $f(a)=a^{-1}$ 则是对于除零外的所有元素都有意义的一元运算．

1.2. 映　射

从一个集合 S 到一个集合 T 的映射是现代数学中的一个

非常基本的概念.

定义. 从集合 S 到集合 T 的映射 α 是对于集合 S 的每个元素 x 指定集合 T 的唯一元素 y 的一个规则. 我们把它记做:

$$\alpha: x \to y \quad 或 \quad y = (x)\alpha.$$

元素 y 叫做 x 在 α 下的像. 如果集合 T 的每个 y 至少是 S 中一个 x 的像, 则就说 α 是从 S 到 T 上[1] 的映射.

从一个集合到自身的映射是特别重要的. 例如平面的旋转可以看作是从平面的点集到自身上的映射. 按照以下的定义, 从集合 S 到自身的两个映射 α 和 β 可以结合起来而产生从 S 到自身的第三个映射.

定义. 给定从集合 S 到自身的两个映射 α 和 β, 我们用以下规则定义从 S 到自身的第三个映射 γ, 如果 $y=(x)\alpha$ 而且 $z=(y)\beta$, 则 $z=(x)\gamma$. 映射 γ 叫做 α 和 β 的乘积而且记做 $\gamma=\alpha\beta$.

这时因为 $y=(x)\alpha$ 和 $z=(y)\beta$ 都是唯一的, 所以 $z=[(x)\alpha]\beta=(x)\gamma$ 对于 S 的每个 x 都有意义而且是 S 的唯一的元素.

定理 1.2.1. 如果用映射的乘积来定义乘法, 则从集合 S 到自身的全体映射满足 $M0$, $M1$ 和 $M3$.

证明. 上面已经说过 $M0$ 是成立的. 让我们来讨论 $M1$. 设 α, β, γ 是三个已知映射. 取 S 的任意元素 x 而且设 $y=(x)\alpha$, $z=(y)\beta$ 和 $w=(z)\gamma$. 那么 $(x)[(\alpha\beta)\gamma]=(z)\gamma=w$, 而且 $(x)[\alpha(\beta\gamma)]=(y)(\beta\gamma)=w$. 因为两个映射 $(\alpha\beta)\gamma$ 和 $\alpha(\beta\gamma)$ 对于 S 的每个 x 都给出相同的像, 所以 $(\alpha\beta)\gamma=\alpha(\beta\gamma)$.

---

1) 请读者注意"从 S 到 (into) T 的映射"和"从 S 到 T 上 (onto) 的映射"的区别. ——译者

为了证明 $M3$ 成立，设 1 是对于 S 的每个 x 使 $(x)\,1=x$ 的映射．那么 1 在下列意义下就是一个单位元素：对于任何映射 α，$\alpha 1 = 1\alpha = \alpha$．

一般地说，$M2$ 和 $M4$ 对于映射不一定成立．但是对于一类重要的映射，即从 S 到自身上的一一映射，$M4$ 成立．

定义．从集合 S 到集合 T 上的映射 α 叫做一一的（我们常常把它记做 1—1），如果 T 的每个元素恰好是 S 的一个元素的像．我们把这样的映射记做：$\alpha: x \rightleftarrows y$，这里 x 是 S 的元素，y 是 T 的元素．这时我们说 S 和 T 的元素的基数[1] 相同．

定理 1.2.2. 从集合 S 到自身上的全体一一映射满足 $M0$，$M1$，$M3$ 和 $M4$．

证明． 因为定理 1.2.1 包括了 $M0$，$M1$ 和 $M3$，我们只要验证 $M4$．如果 $\alpha: x \rightleftarrows y$ 是从 S 到自身上的一一映射，则根据定义，对于 S 的每个 y，恰好存在 S 的一个 x 使得 $y=(x)\alpha$．这样对于每个 y 就规定了唯一的 x，这个规定决定了从 S 到自身上的一个一一映射 $\tau: y \rightleftarrows x$．从 τ 的定义得出，对于 S 的每个 x，$(x)(\alpha\tau)=x$，又对于 S 的每个 y，$(y)(\tau\alpha)=y$．因此 $\alpha\tau=\tau\alpha=1$，因而 τ 是具有 $M4$ 中 α^{-1} 的性质的映射．

我们把从一个集合到它自身上的一一映射叫做置换．要是已知集合是有限的，为了表示一个置换，可以把这集合的元素排成一行而且把它们的像记在下面．因而 $\alpha=\begin{pmatrix}1, & 2, & 3\\ 2, & 3, & 1\end{pmatrix}$

1）关于基数的讨论，参看 Birkhoff and MacLane[1]，第 356 页．这个概念以及本书中其他类似于它的概念都请参考所提出的文献．（译者按：集合的元素的基数也叫做集合的势．）

和$\beta = \begin{pmatrix}1, 2, 3\\1, 3, 2\end{pmatrix}$是集合 $S(1, 2, 3)$ 的两个置换. 它们的乘积就定义为置换 $\alpha\beta = \begin{pmatrix}1, 2, 3\\3, 2, 1\end{pmatrix}$. 注意这里给出的置换相乘的规则是从左到右的. 有些作者定义置换乘积是从右到左地相乘的.

1.3. 群和若干有关体系的定义

我们看到,作为单个的运算,加法和乘法满足同样一些定律. 这些定律除交换律外,还都被从一个集合到自身上的一一映射的相乘规则所满足. 这些一一映射所服从的定律正是我们用来定义群的定律.

定义(群的第一个定义). 群 G 是这样的元素集合 $G(a, b, c, \cdots)$, 它具有叫做"乘法"的一个二元运算, 满足:

$G0$. 闭合律. 对于 G 的每一对有序的元素 a 和 b, 乘积 $ab = c$ 存在而且是 G 的唯一的元素.

$G1$. 结合律. $(ab)c = a(bc)$.

$G2$. 单位元素的存在. 存在元素 1, 使得对于 G 的每个 a, 都有 $1a = a1 = a$.

$G3$. 逆的存在. 对于 G 的每个 a, 存在 G 的元素 a^{-1}, 使得 $a^{-1}a = aa^{-1} = 1$.

这些定律中有多余的. 我们可以略去 $G2$ 和 $G3$ 的一半, 而把它们换成:

$G2^*$. 存在元素 1, 使得对于 G 的每个 a, $1a = a$.

$G3^*$. 对于 G 的每个 a, 存在 G 的元素 x, 使得 $xa = 1$.

让我们来证明从这两个定律可以导出 $G2$ 和 $G3$. 对于已知的 a, 根据 $G3^*$, 设

$$xa = 1 \quad \text{和} \quad yx = 1.$$

于是我们有

$$ax=1(ax)=(yx)(ax)=y[x(ax)]=y[1x]=yx=1,$$

因而 $G3$ 成立．再有，

$$a = 1a = (ax)a = a(xa) = a1,$$

因而 $G2$ 也成立．

单位元素 1 和逆 a^{-1} 的唯一性很容易确立（参看习题 13)．我们当然还可以把 $G2$ 和 $G3$ 换成这样的假设：使得 $a1 = a$ 和 $ax = 1$ 的 1 和 x 存在．但是如果假设它们满足 $a1 = a$ 和 $xa = 1$，情况就有些不同[1]．

可以有好多种方法把一个序列 $a_1a_2\cdots a_n$ 加括弧以便逐步用二元乘积来计算它的值．当 $n = 3$ 时恰好有两种加括弧的方法，那就是 $(a_1a_2)a_3$ 和 $a_1(a_2a_3)$，而结合律断定这两个乘积是相等的．结合律的一个重要的推论是广义结合律．

把序列 $a_1a_2\cdots a_n$ 加括弧以便逐步用二元乘积来计算它的值的所有各种方法产生同样的一个值．

对 n 施行归纳法，容易证明广义结合律是结合律的推论（参看习题 1）．

可以给出另一个定义，它并未明白地假设单位元素的存在．

定义（群的第二个定义）．群 G 是这样的元素集合 $G(a, b, c, \cdots)$．它满足：

1）对于 G 的每一对有序的元素 a 和 b，二元乘积 ab 有定义，使得 $ab = c$ 是 G 的唯一的元素．

2）对于 G 的每个元素 a，一元运算"逆" a^{-1} 有定义，使得 a^{-1} 是 G 的唯一的元素．

1）参看H. B. Mann[1]．

3) 结合律. $(ab)c = a(bc)$.

4) 逆律. $a^{-1}(ab) = b = (ba)a^{-1}$.

容易验证满足第一个定义的全体公理的任何集合也满足第二个定义的公理. 为了证明逆命题，假设第二个定义的公理成立，考虑下面的等式：

$$a^{-1}a = [(a^{-1}a)b]b^{-1} = (a^{-1}a)(bb^{-1})$$
$$= a^{-1}[a(bb^{-1})] = bb^{-1}.$$

当 $a = b$ 时我们有 $a^{-1}a = aa^{-1}$，因而对于 G 的每个 a，元素 $a^{-1}a = aa^{-1}$ 是相同的. 我们把这个元素叫做"1"，于是 $G3$ 成立. 再有，

$$1b = (a^{-1}a)b = a^{-1}(ab) = b,$$

和

$$b1 = b(aa^{-1}) = (ba)a^{-1} = b,$$

即 $G2$ 也成立. 因此群的两个定义是等价的.

还有群的第三个定义如下：

定义（群的第三个定义）. 群 G 是这样的元素集合 $G(a, b, \cdots)$，它具有二元运算 a/b，满足：

$L0$. 对于 G 的每一对有序的元素 a 和 b，a/b 有定义，使得 $a/b = c$ 是 G 的唯一的元素.

$L1$. $a/a = b/b$.

$L2$. $a/(b/b) = a$.

$L3$. $(a/a)/(b/c) = c/b$.

$L4$. $(a/c)/(b/c) = a/b$.

利用这个运算，我们用下列规则定义一元运算——逆 b^{-1}：

$$b^{-1} = (b/b)/b.$$

于是利用 $L3$ 和 $L2$，我们有

$$(b^{-1})^{-1} = (b^{-1}/b^{-1})/b^{-1} = (b^{-1}/b^{-1})/[(b/b)/b]$$
$$= b/(b/b) = b.$$

现在我们再用下列规则定义二元运算——乘积：

$$ab = a/b^{-1}.$$

于是 $a/b = a/(b^{-1})^{-1} = ab^{-1}$. 我们用 1 表示由 $L1$ 确定的 $a/a = b/b$ 的公共值. 于是 $L1$ 变成 $aa^{-1} = 1$, 同时对于任何 a 还有 $1 = a^{-1}(a^{-1})^{-1} = a^{-1}a$. 因而第一个定义的 $G3$ 成立. 在 $b^{-1} = (b/b)/b$ 里, 令 $b = 1$, 就有 $1^{-1} = 11^{-1}$, 因而 $1 = 1/1 = 11^{-1} = 1^{-1}$. 于是 $L2$ 变成 $a1^{-1} = a1 = a$. 根据定义, $b^{-1} = 1/b = 1b^{-1}$, 只要令 $b = a^{-1}$, 这就给出 $(a^{-1})^{-1} = 1(a^{-1})^{-1}$ 或 $a = 1a$. 因此第一个定义的 $G2$ 成立. 现在 $L3$ 变成 $1(bc^{-1})^{-1} = cb^{-1}$, 因而 $(bc^{-1})^{-1} = cb^{-1}$. 在 $L4$ 里, 令 $a = x$, $b = 1$, $c = y^{-1}$; 于是 $(xy)(1y)^{-1} = x1^{-1} = x$, 即 $(xy)y^{-1} = x$. 现在对于任何 x, y, z, 令 $a = xy, b = z^{-1}$, $c = y$. 那么 $ac^{-1} = (xy)y^{-1} = x$. 又 $L4$ 可以改写成 $(ac^{-1})(bc^{-1})^{-1} = ab^{-1}$, 即 $(ac^{-1})(cb^{-1}) = ab^{-1}$. 这个等式用 x, y, z 写出是 $x(yz) = (xy)z$, 这就是结合律 $G1$. 因此从群的这个定义可以导出第一个定义. 反之, 根据第一个定义, 只要令 $ab^{-1} = a/b$, 我们容易验证 $L0, L1, L2, L3, L4$ 都成立. 因此这两个定义是等价的.

还有一些只满足群的一部分公理的代数体系. 以下是主要的几种:

定义. 拟群 Q 是这样的元素体系 $Q(a, b, c, \cdots)$, 在其中定义了二元乘积运算 ab, 使得在 $ab = c$ 中, Q 的元素 a, b, c 的任何两个都能唯一地决定第三个.

定义. 络是具有单位元素 1 的拟群, 使得对于任何元素 a, $1a = a1 = a$.

定义. 半群是这样的元素体系 $S(a, b, c, \cdots)$, 它具有二元乘积运算 ab, 使得 $(ab)c = a(bc)$.

群自然满足所有这些定义. 库罗什曾经指出, 可以把群

定义为既是半群又是拟群的集合。作为半群，$G0$ 和 $G1$ 成立. 设对于某个 b，t 是使 $tb=b$ 的唯一元素，再设 y 是在 $by=a$ 中由 b 和 a 决定的元素. 那么 $(tb)y=by$，因而 $t(by)=by$，即对于任何 a 都有 $ta=a$，因此 $G2^*$ 成立. 在拟群中 $G3^*$ 也成立. 可是我们已经证明过了，这些性质就决定了群.

具有可逆性质的拟群是指具有二元乘积和一元逆满足

$$a^{-1}(ab)=b=(ba)a^{-1}$$

的体系，上述等式就表示可逆性质. 我们必须证明可逆拟群中的乘积决定一个拟群. 如果 $ab=c$，则我们有 $b=a^{-1}(ab)=a^{-1}c$ 和 $a=(ab)b^{-1}=cb^{-1}$. 因而不仅 a 和 b 唯一地决定 c；而且给定了 c 和 a，最多有一个 b，又给定了 c 和 b，最多有一个 a. 记 $a(a^{-1}c)=w$. 那么 $a^{-1}[a(a^{-1}c)]=a^{-1}w$，因而 $a^{-1}c=a^{-1}w$. 于是 $(a^{-1})^{-1}(a^{-1}c)=(a^{-1})^{-1}(a^{-1}w)$，因而 $c=w$. 因此 $a(a^{-1}c)=c$，同理 $(cb^{-1})b=c$，所以这体系是拟群. 我们注意到可逆拟群不一定是络. 给了三个元素 a，b，c 和关系式 $a^2=a$，$ab=ba=c$，$b^2=b$，$bc=cb=a$，$c^2=c$，$ca=ac=b$，我们发现可以取每个元素作为它自己的逆而得到一个可逆拟群，但是它没有单位元素.

1.4. 子群，同构，同态

群 G 元素的子集可以对于 G 中的乘法也成为群. 这样的元素集合 H 叫做 G 的**子群**.

在任何群 G 里，单位元素 1 满足 $1^2=1$. 反之，如果 x 是 G 的元素，使得 $x^2=x$，则 $x=x^{-1}(x^2)=x^{-1}x=1$. 因此，由于子群 H 的单位元素满足 $x^2=x$，它必须同时是整个群 G 的单位元素.

定理 1.4.1. 群 G 的子集 H 在下列两个条件成立时是子群:

$S1$. 如果 $h_1 \in H$, $h_2 \in H$, 则 $h_1 h_2 \in H$.

$S2$. 如果 $h_1 \in H$, 则 $h_1^{-1} \in H$.

证明. 这两个性质保证 $G0$, $G2$, $G3$ 在 H 内成立. 而由于 H 内的乘法就是 G 内的乘法, $G1$ 在 H 内也成立.

在一对群之间有各种值得讨论的关系. 第一个这种关系是所谓同构.

定义. 从群 G 到群 H 上的一一映射 $G \rightleftarrows H$ 叫做同构, 假如从 $g_1 \rightleftarrows h_1$ 和 $g_2 \rightleftarrows h_2$ 得出 $g_1 g_2 \rightleftarrows h_1 h_2$.

例1. 因为一个集合的全体置换组成群 (定理 1.2.2), 所以满足 $S1$ 和 $S2$ 的任何置换集合是群, 它是全体置换的群的子群. 例如, 让我们来讨论以下两个这样的子群:

$$\begin{array}{ll} G_1 & G_2 \\ x_1 = \begin{pmatrix} 1, 2, 3 \\ 1, 2, 3 \end{pmatrix} & y_1 = \begin{pmatrix} 1, 2, 3, 4, 5, 6 \\ 1, 2, 3, 4, 5, 6 \end{pmatrix} \\ x_2 = \begin{pmatrix} 1, 2, 3 \\ 2, 3, 1 \end{pmatrix} & y_2 = \begin{pmatrix} 1, 2, 3, 4, 5, 6 \\ 2, 3, 1, 6, 4, 5 \end{pmatrix} \\ x_3 = \begin{pmatrix} 1, 2, 3 \\ 3, 1, 2 \end{pmatrix} & y_3 = \begin{pmatrix} 1, 2, 3, 4, 5, 6 \\ 3, 1, 2, 5, 6, 4 \end{pmatrix} \\ x_4 = \begin{pmatrix} 1, 2, 3 \\ 1, 3, 2 \end{pmatrix} & y_4 = \begin{pmatrix} 1, 2, 3, 4, 5, 6 \\ 4, 5, 6, 1, 2, 3 \end{pmatrix} \\ x_5 = \begin{pmatrix} 1, 2, 3 \\ 3, 2, 1 \end{pmatrix} & y_5 = \begin{pmatrix} 1, 2, 3, 4, 5, 6 \\ 5, 6, 4, 3, 1, 2 \end{pmatrix} \\ x_6 = \begin{pmatrix} 1, 2, 3 \\ 2, 1, 3 \end{pmatrix} & y_6 = \begin{pmatrix} 1, 2, 3, 4, 5, 6 \\ 6, 4, 5, 2, 3, 1 \end{pmatrix} \end{array}$$

如果我们把 G_1 的 x_i 映成 G_2 的 y_i, 我们发现在任何情况下乘积总对应于乘积. 因此 G_1 和 G_2 是同构的.

更通常遇到的从群G到群H上的保持乘积的映射常常是多对一的，我们把它叫做同态.

定义. 从群G到群H上的映射 $G\to H$ 叫做同态，如果从 $g_1\to h_1$ 和 $g_2\to h_2$ 得到 $g_1g_2\to h_1h_2$.

在同态 $G\to H$ 下，设 1 是G的单位元素而且 $1\to e$，这里 e 在H里. 那么 $1^2\to e^2$. 因为 $1^2=1$，所以 $e^2=e$. 因此 e 是H的单位元素. 又如果 $g\to h$ 而且 $g^{-1}\to k$，那么 $gg^{-1}\to hk$，因而 $1\to hk=e$. 因此 $k=h^{-1}$，即这个映射把逆映成逆. 容易看出一一的同态是同构.

例 2. 如果 G_1是例 1 中的置换群，而H是由 1 和 -1 两个实数组成的乘法群，那么我们有一个同态:

$$x_1\to 1 \qquad x_4\to -1$$
$$x_2\to 1 \qquad x_5\to -1$$
$$x_3\to 1 \qquad x_6\to -1$$

置换群不仅本身是有趣的，而且任何群总同构于一个置换群.

定理 1.4.2（凯雷）. 任何一个群G总同构于它自己的元素的一个置换群.

证明. 对于每个 $g\in G$，定义映射 $R(g): x\to xg$ 对于所有 $x\in G$. 对于固定的 g，这是从G到自身上的映射，因为对于给定的 y，$yg^{-1}\to(yg^{-1})g=y$. 它还是一一的，因为从 $x_1g=x_2g$ 得出 $x_1=x_2$. 因此对于每个 g，$R(g)$ 都是置换. 映射 $R(g_1)\ R(g_2)$ 是映射 $x\rightleftarrows(xg_1)g_2=x(g_1g_2)$，因而 $R(g_1)\,R(g_2)=R(g_1g_2)$. 其次，在 $R(g_1)$ 下，$1\rightleftarrows g_1$，而在 $R(g_2)$下，$1\rightleftarrows g_2$. 因此如果 $g_1\neq g_2$，则 $R(g_1)\neq R(g_2)$. 这说明映射 $g\rightleftarrows R(g)$ 是同构. 再有我们看到 $g(1)=I$ 是恒同映射，而且 $R(g^{-1})R(g)=I$，所以 $R(g^{-1})=[R(g)]^{-1}$.

置换 $R(g): x\rightleftarrows xg$ 叫做G的右正则表示. 我们也可以

讨论置换 $L(g)$：$x \rightleftarrows gx$，即 G 的左正则表示．我们发现 $L(g)$ 是反同构于 G 的．这是说映射 $g \rightleftarrows L(g)$ 是一一的，但是是逆序相乘的，即 $L(g_1g_2) = L(g_2)L(g_1)$．

如果我们有 G 的一组子群 H_j，这里 j 遍历一个指标集 J，则 G 中属于每一个 H_j 的元素的集合满足 S1 和 S2，因而是一个子群 H，它叫做 H_j 的交．我们把它记做：$H = \bigcap_j H_j$．其次，每个 g_i 属于某个 H_j 的全体有限乘积 $g_1g_2\cdots g_s$ 的集合也满足 S1 和 S2．这个集合形成的子群 T 叫做 H_j 的并，记做 $T = \bigcup_j H_j$．两个子群 H 和 K 的交和并我们分别记做 $H \cap K$ 和 $H \cup K$．这个记号是与格论里的同样记号协调的，而且将在第八章里作更充分的讨论．

群的元素的任意集合说成群的子集[1]．如果 A 和 B 是群 G 的两个子集，我们用 AB 表示由 $a \in A$ 和 $b \in B$ 的全体元素 ab 组成的子集，而且把 AB 叫做 A 和 B 的乘积．我们容易验证子集的乘法满足结合律 $(AB)C = A(BC)$．

如果 K 是群 G 的任意子集，我们用 $\{K\}$ 表示由所有这种有限乘积 $x_1\cdots x_n$ 组成的子群，这里每个 x_i 是 K 的一个元素或 K 的一个元素的逆．我们说 $\{K\}$ 由 K 生成．容易看出 $\{K\}$ 包含在 G 的任何包含 K 的子群中．

1.5. 傍系．拉格朗日定理．循环群．指数

给了群 G 和它的子群 H．对于所有的 $h \in H$ 和固定的 $x \in G$，全体元素 hx 的集合叫做 H 的一个左傍系[2] 而且记做 Hx．同理，对于所有 $h \in H$，元素 xh 的集合叫做 H 的一个右

1) 原文引用一个术语叫做复（complex）．——译者

2) 傍系（coset）采用科学出版社《英汉数学词汇》（1974年版）所定的名词，在不少近世代数书上也叫做陪集．——译者

傍系 xH.

定理 1.5.1. H 在 G 内的两个左(右)傍系是不相交的或全合的元素集合. H 的左(右)傍系与 H 的基数相同.

证明. 如果傍系 Hx 和 Hy 没有公共的元素,就不需要证明什么了. 因此假定 $z\in Hx$, $z\in Hy$. 那么 $z=h_1x=h_2y$. 这时 $x=h_1^{-1}h_2y$ 而且 $hx=hh_1^{-1}h_2y=h'y$, 因而 $Hx\subseteq Hy$. 同理 $hy=hh_2^{-1}h_1x=h''x$, 因而 $Hy\subseteq Hx$. 于是 $Hx=Hy$, 即这两个集合全合. 对于右傍系可以作同样的证明. 一一对应 $h\rightleftarrows hx$, $h\rightleftarrows xh(h\in H)$ 指出 H, Hx 和 xH 的基数相同.

元素 $x=x1=1x$ 属于傍系 xH 和 Hx, 它就叫做傍系的代表. 根据定理 1.5.1, 任何元素 $u\in Hx$ 都可以取作代表, 因为 $Hu=Hx$. 因此 $H=H1=1H$ 是它自己的一个傍系, 而且当一个子群被看作为自己的傍系时, 取单位元素作为代表常常是方便的(而在某种规定下还是必要的). 我们用

$$G=H+Hx_2+\cdots+Hx_r \tag{1.5.1}$$

表示傍系 H, Hx_1, $\cdots$, Hx_r 是不相交的而且穷举了 G 的元素. 这里所写的加法只是一种规定的记号而不能识为是一种运算.

因为 $(Hx)^{-1}$ (hx 形状的元素的逆的集合) 相当于 $x^{-1}H$, 又 $(yH)^{-1}=Hy^{-1}$, 在 H 的左右傍系之间有一个一一对应. 因此从 (1.5.1) 得出

$$G=H+x_2^{-1}H+\cdots+x_r^{-1}H. \tag{1.5.2}$$

子群 H 在群 G 内的左或右傍系的集合的基数 r 叫做 H 在 G 内的指数, 而且记做 $[G:H]$. 群 G 的元素的基数叫做 G 的阶. 单独一个单位元素是一个子群, 它的傍系只包含一个元素. 因而群的阶是单位元素子群的指数.

定理 1.5.2 (拉格朗日定理). 群 G 的阶等于子群 H 的阶和 H 在 G 内的指数的乘积.

证明. H 在 G 内的 $r=[G:H]$ 个不相交的傍系中每一个所包含的元素个数都与 H 相同，即是 H 的阶.

设 H 是 G 的子群，K 是 H 的子群，令

$$G = H + Hx_2 + \cdots + Hx_s,$$
$$H = K + Ky_2 + \cdots + Ky_r.$$

那么对于 $g\in G$, $g=hx_j$, $h\in H$ 的方式是唯一的，同理 $h=ky_i$, $k\in K$ 的方式也是唯一的．因此 K 在 G 内的傍系由 Ky_ix_j, $i=1,\cdots,r$, $j=1,\cdots,s$ 给定．这是因为如果这样两个傍系相合，它们就要属于 H 的同一个傍系，因而就要有相同的 x_j．在右边乘上 x_j^{-1}，我们看到它们还要有相同的 y_i．因此 Ky_ix_j 都是不同的，而 K 在 G[1] 内的傍系就由它们给出．这也就证明了下列定理[2]:

定理 1.5.3. 如果 $G\supseteq H\supseteq K$，则 $[G:K]=[G:H][H:K]$.

如果群 G 的每个元素都是某个固定元素 b 的方幂 b^i，则 G 叫做循环群．如果我们记 $(b^{-1})^r=b^{-r}$，则根据结合律和归纳法可以证明，对于任何整数方次 m 和 t，$b^mb^t=b^{m+t}$．如果 b 的所有方幂都是不同的，则循环群是无限阶的，而且它同构于全体整数的加法群，这些整数就是生成元素 b 的方次数．如果并非所有方幂都不相同，设 $b^m=b^t$, $m>t$．那么 $b^{m-t}=1$，这里 $m-t$ 是正的．设 $n>0$ 是使 $b^n=1$ 的最小正整数．那么我们立刻知道群的元素是 $1, b,\cdots,b^{n-1}$，而且当 $0\leqslant r,s<n$ 时，如果 $r+s<n$，则 $b^rb^s=b^{r+s}$，又如果 $r+s\geqslant n$，则 $b^rb^s=b^{r+s-n}$．由此我们可以直接验证，对于每个正整数 n，在同构下只有唯一的 n 阶循环群．这也就是整数取模 n 的加法群．因此，对于由一个元素 b 生成的循环群，它的阶或是无限的或是某个整数 n，在后一情形 n 是

1) 原书错印成 H.——译者

2) 定理 1.5.3 当 K 是单位元素子群时就是定理 1.5.2.——译者

使$b^n=1$的最小正整数．我们定义元素 b 的阶为由它生成的循环群 $\{b\}$ 的阶．

群 G 的子群的本质和个数当然在刻画 G 本身时大有价值．但是如果G除本身和单位元素群外没有其他子群，则就没有刻划它的结构的真子群． 在这种情形下我们可以给出G的一个很简单的直接描述．

定理 1.5.4. 设G是阶大于一的群．那么 G 除本身和单位元素群外没有其他子群，必要而且只要G是素数阶的循环群．

证明．根据假设，如果 $b\neq 1$ 是G的元素，则由 b 生成的循环群不是单位元素群，因而必须是整个群 G．如果 b 是无限阶的，则 b^2 生成由元素 b^{2i} 组成的真子群．因此 b 是有限阶的，设 b 的阶是 n，于是 $b^n=1$．如果 n 不是素数，那么 $n=uv$，这里 $u>1$，$v>1$．于是 b^v 的方幂组成 v 阶的真子群．因此 n 是素数而G是素数阶的循环群．反之根据拉格朗日定理，素数阶的群不会包含不是单位元素群和整个群的子群．

关于子群的指数有以下的基本关系．

定理 1.5.5. 关于指数的不等式． $[A\cup B:B]\geqslant[A:A\cap B]$．

证明．设 $A\cap B=D$ 和 $A=D1+Dx_2+\cdots+Dx_r$．那么我们可以断定傍系 $B1$，$Bx_2,\cdots$，Bx_r在 $A\cup B$ 内全不相同．因为如果 $Bx_i=Bx_j$，$j\neq i$，则 $x_j=bx_i$，这里 $b\in B$．但是这时 x_i 和 x_j 都属于 A，所以对于这个 b 也有 $b\in A$，因而 $b\in A\cap B=D$；于是傍系 Dx_j 和 Dx_i 就有公共的元素 $x_j=bx_i$ 而与假设矛盾了．因此B在 $A\cup B$ 内的不同的傍系至少有 $A\cap B$ 在A内的不同的傍系那么多，这就证明了不等式．

定理 1.5.6. 指数的等式 如果$[A\cup B:B]$和$[A\cup B:A]$都是有限的而且是互素的，则 $[A\cup B:B]=[A:A\cap B]$ 和

$[A \cup B : A] = [B : A \cap B]$.

证明. 根据定理 1.5.3，

$$[A \cup B : A \cap B] = [A \cup B : B][B : A \cap B]$$
$$= [A \cup B : A][A : A \cap B].$$

又根据定理 1.5.5，$[A \cup B : B] \geqslant [A : A \cap B]$，但是从上面的等式还得出 $[A \cup B : B]$ 整除 $[A : A \cap B]$，因为它与 $[A \cup B : A]$ 是互素的. 因此 $[A \cup B : B] = [A : A \cap B]$，同理 $[A \cup B : A] = [B : A \cap B]$.

1.6. 共轭者和共轭类

设 G 是一个群而 S 是 G 的元素的任意集合. 那么对于固定的 $x \in G$，形状 $x^{-1}sx (s \in S)$ 的元素集合 S' 叫做 S 在 x 下的变形，而且记做 $S' = x^{-1}Sx$ 或 $S' = S^x$.

引理 1.6.1. S 和 S^x 包含同样个数的元素.

证明. $s \rightleftarrows x^{-1}sx$ 是一一对应，因为 $s \to x^{-1}sx = s'$ 和 $s' \to xs'x^{-1} = x(x^{-1}sx)x^{-1} = s$ 都是映射.

如果 S 和 S' 是 G 的两个子集，H 是 G 的子群，而且存在某个 $x \in H$，使得 $S' = S^x$，则我们说 S 和 S' 在 H 下共轭. 如果 $S' = x^{-1}Sx$，则 $S = (x^{-1})^{-1}S'x^{-1}$. 其次，如果 $S'' = y^{-1}S'y$，则 $S'' = y^{-1}x^{-1}Sxy = (xy)^{-1}S(xy)$. 又因为显然有 $S = 1^{-1}S1$，所以在 H 下共轭的关系是自反的、对称的和传递的，即是一种等价关系. 我们把共轭于已知的 S 的全体 S' 的集合叫做共轭类. 从 $(x^{-1}sx)^{-1} = x^{-1}s^{-1}x$ 和 $x^{-1}s_1x \cdot x^{-1}s_2x = x^{-1}(s_1s_2)x$ 得出:

引理 1.6.2. 共轭于一个子群的任何集合也是子群.

如果 $x^{-1}Sx = S$，则 $S = xSx^{-1}$. 如果还有 $y^{-1}Sy = S$，则 $S = (xy)^{-1}S(xy)$. 因此，使 $S^x = S$ 的 $x \in H$ 的集合是 H 的子

群，我们把它叫做 S 在H内的正规化子而且记做$N_H(S)$．再有，使$x^{-1}sx=s$对于所有$s\in S$都成立的$x\in H$的集合同样可以证明是H的子群，我们把它叫做S在H内的中心化子而且记做$C_H(S)$[或者用德文称呼而记做$Z_H(S)$]．注意当S只包含一个元素时，中心化子和正规化子是相合的；而且总有$C_H(S)\subseteq N_H(S)$．当$H=G$时通常只说S的正规化子和中心化子．G在G内的中心化子Z叫做G的中心．

定理 1.6.1. S 在H下的共轭者的个数等于 S 在H内的正规化子在 H 内的指数$[H:N_H(S)]$.

证明. 为了简单起见，记$N_H(S)=D$，而且设

$$H=D+Dx_2+\cdots+Dx_r, r=[H:N_H(S)].$$

那么 $x^{-1}Sx=y^{-1}Sy$ $(x, y\in H)$，必要而且只要 $S=(yx^{-1})^{-1}S(yx^{-1})$；即$yx^{-1}\in D$或$y\in Dx$.因此$S$在$H$下的两个共轭者相同，必要而且只要用作变形的元素属于D的同一个左傍系．因此不同的共轭者的个数等于D在H内的指数，这就是所要证明的．

如果S只包含一个元素 s，它在G下的共轭类是G的元素的集合．因此G的元素的共轭类形成G的一个剖分，我们记做

$$G=C_1+C_2+\cdots+C_s, \qquad (1.6.1)$$

这里C_i表示不相交的共轭类，而且G的每一个元素恰好只是一个共轭类的元素．单位元素1本身总是一个共轭类．根据定理 1.6.1，任何共轭类C_i的元素个数是一个子群的指数．因此它是群的阶的约数．

1.7. 二 重 傍 系

给了群G和两个子群H和K（不一定是不同的），对于G

的某个固定的元素 x，元素集合 HxK 叫做**二重傍系**．像普通的傍系一样，我们可以证明：

引理 1.7.1. 两个二重傍系 HxK 和 HyK 或是不相交的，或是全合的．

证明．如果 $z = h_1xk_1 = h_2yk_2$，则 $hxk = hh_1^{-1}h_2yk_2k_1^{-1}k$，因而 $HxK \subseteq HyK$，同理 $HyK \subseteq HxK$．

二重傍系 HxK 包含 H 的 Hxk 形状的所有左傍系和 K 的 hxK 形状的所有右傍系．此外，HxK 显然由 H 的一些完整的左傍系组成，也由 K 的一些完整的右傍系组成．

定理 1.7.1. 包含在 HxK 里的 H 的左傍系数等于 $[K: K\cap x^{-1}Hx]$，包含在 HxK 里的 K 的右傍系数等于 $[x^{-1}Hx: K\cap x^{-1}Hx]$．

证明．利用规则 $hxk \rightleftarrows x^{-1}hxk$，我们使 HxK 的元素与 $x^{-1}HxK$ 的元素成 1—1 对应．这个对应给出在 HxK 内的 H 的左傍系 Hxk 和在 $x^{-1}HxK$ 内的 $x^{-1}Hx$ 的左傍系 $x^{-1}Hx\cdot k$ 之间的 1—1 对应，也给出 K 在 HxK 内的右傍系 hxK 和 K 在 $x^{-1}HxK$ 内的右傍系 $x^{-1}hxK$ 的 1—1 对应．我们记 $x^{-1}Hx = A$ 和 $A\cap K = D$．于是如果 $A = 1\cdot D + u_2D + \cdots + u_rD$，$r = [A: D]$，则 $u_i \in A$，因而 $K, u_2K, \cdots, u_rK$ 是在 AK 内的 K 的右傍系．它们都是不同的，因为如果 $u_iK = u_jK$，则 $u_iu_j^{-1} \in K$，而由于 u_i，$u_j \in A$，由此就将有 $u_i^{-1}u_j \in D$，因而 $u_iD = u_jD$，这是与假设矛盾的．在 AK 内 K 的每个右傍系有形状 aK，这里 $a\in A$ 有形状 u_id，$d\in D$．但是 $u_idK = u_iK$．因此在 AK 内 K 的右傍系数等于 $[A:D] = [x^{-1}Hx : x^{-1}Hx\cap K]$，再根据 1—1 对应，这就是在 HxK 内的 K 的右傍系数．同理可以证明在 AK 内 A 的左傍系数等于 $[K: D] = [K: x^{-1}Hx\cap K]$，而根据 1—1 对应，这就是在 HxK 内的 H 的左傍系数．

1.8. 关于无限群的附注

关于群的很多定理并不涉及这群是否是有限群的问题. 但是在有的时候对于有限群和无限群结论可以绝然不同，而且即使结论相同，证明的方法也常常不同.

无限群 G 可以具有某些有限的性质. 以下是这种性质中的几个重要的性质:

1) G 是有限生成的[1].

2) G 是周期群，即 G 的元素都是有限阶的.

3) G 满足极大条件: 不同子群的每一个递升链 $A_1 \subset A_2 \subset A_3 \subset \cdots$ 必定是有限的.

4) G 满足极小条件: 不同子群的每一个递降链 $A_1 \supset A_2 \supset A_3 \supset \cdots$ 必定是有限的.

无限群 G 说成是局部地具有某个性质，假如每一个有限生成的子群都具有这个性质. 群 G 的同态像族 H_i 叫做 G 的剩余族，假如对于 G 的每个 $g \neq 1$，至少有一个 H_i，这个 g 在其中的像不是单位元素. 我们说 G 剩余地具有某个性质，如果 G 有一个剩余族的同态像，它们全都具有这个性质.

定理 1.8.1. 群 G 满足极大条件，必要而且只要 G 和 G 的每个子群都是有限生成的.

证明 设 H 是 G 的不是有限生成的子群. 我们可以逐次地构造 H 的不同子群的无限递升序列 $\{h_1\} \subset \{h_1, h_2\} \subset \cdots \subset \{h_1, \cdots, h_i\} \subset \cdots$，只要任意选取 h_1，然后逐次地选取 H 的不在 $\{h_1, \cdots, h_{i-1}\}$ 里的一个元素作为 h_i. 因为 H 不会是有限生成群 $\{h_1, \cdots, h_{i-1}\}$，所以这样一个 h_i 总是存在的. 反

---

1) 即 G 由有限个元素生成. ——译者

之，假定 G 和它的所有子群都是有限生成的．设 $B_1 \subseteq B_2 \subseteq B_3 \subseteq \cdots$ 是 G 的子群的递升链．我们只要证明在这个链的某一段以后所有的子群都是相同的，也就证明了不同子群的无限递升链不存在．考虑所有的 $b \in B_i$，这里 B_i 是链中的群，这种 b 的集合形成 G 的一个子群 B，因为如果 $b \in B_i$ 和 $b' \in B_j$，则 b 和 b' 就都属于任何 $B_k(k \geqslant i, k \geqslant j)$，因而它们的乘积和逆也都在 B_k 里．

根据假设 B 是有限生成的，设生成元素是 $x_1, \cdots, x_n$．设 B_{i_1} 是包含 x_1 的第一个 B_i，一般地设 B_{i_k} 是包含 x_k 的第一个 B_i，$k = 1, \cdots, n$．那么如果 m 是 $i_1, \cdots, i_n$ 中的最大的，则 B_m 就包含了全体 $x_1, \cdots, x_n$，因而 $B = B_m = B_{m+1} = \cdots$，即链中从 B_m 开始的所有的群都等于 B．以后我们将会遇到具有不是有限生成的子群的有限生成群．

定理 1.8.2. 满足极小条件的群 G 是周期群．

证明 如果 G 包含无限阶的元素 b，则 $\{b\} \supset \{b^2\} \supset \{b^4\} \supset \cdots \supset \{b^{2i}\} \supset \cdots$ 就是不同子群的无限递降链．

在无限群内不能对它的阶施行有限归纳法，因而必须有某种东西来代替对于有限群极有价值的这种证明方法．引入某些关于集合和顺序的更广义的公理是实现这种代替的一个途径．假定对于集合 $S(a, b, c, \cdots)$ 的元素有了一个顺序关系 $a \leqslant b$．这个顺序可以满足下列公理中的某几个：

01）如果 $a \leqslant b$ 和 $b \leqslant a$，则 $a = b$.

02）如果 $a \leqslant b$ 和 $b \leqslant c$，则 $a \leqslant c$.

03）对于任何两个 a 和 b，不是 $a \leqslant b$，就是 $b \leqslant a$.

04）S 的任何非空子集 T 都有一个第一元素 x_1，即对于每个 $t \in T$ 都有 $x_1 \leqslant t$ 的元素 x_1.

如果前两个公理成立，我们说这个顺序是一个偏序．如果前三个公理成立，我们说这个顺序是一个全序．如果全部

四个公理都成立，我们说这个顺序是一个良序．我们可以导入良序公理：任何集合 S 都能成为良序的．我们用 $a < b$ 表示 $a \leqslant b$ 而 $a \neq b$．

在良序集合里可以用超限归纳法来证明命题．这是这样进行的：把 S 的第一元素记做 1．于是，如果 $P(a)$ 是关于 S 的元素的命题而且 $P(1)$ 成立，又如果从 $P(x)$ 对于所有 $x < a$ 成立得出 $P(a)$ 也成立，则结论是 $P(b)$ 对于所有 $b \in S$ 都成立．设 T 是 S 的子集，使得对于 $t \in T$，$P(t)$ 不成立．如果 T 是不空的，它包含一个第一元素 c．于是或者 $c = 1$，或者 $P(x)$ 对于所有 $x < c$ 都成立．不论那一种情形都能得出 $P(c)$ 成立而与 c 在 T 内的选取相矛盾．因此 T 必须是空的而 $P(b)$ 对于所有 $b \in S$ 都成立．我们还看出在良序集合里任何递降序列 $a_1 > a_2 > a_3 > \cdots$ 必定是有限的，因为它包含第一元素．

在逻辑上等价于良序公理的另一公理是左恩引理．这也是论述集合内的顺序的．

引理 1.8.1（左恩引理）． 给了一个偏序集合 S．假定 S 的每个全序子集在 S 内都有上界（下界）．那么 S 具有一个极大的（极小的）元素．这里如果 U 是 S 的子集，则所谓 U 的上界 b 是对于所有 $u \in U$ 都有 $b \geqslant u$ 的元素．极大元素 w 是指除它本身外无其他上界的元素．把顺序关系反过来，可以同样地定义下界和极小元素．

假定我们考虑群 G 的子群集合，用 $A \subseteq B$ 表示 A 是 B 的子群来确定一个偏序．那么在这子群集合的一个全序子集的全体子群里的所有元素的集合本身是一个子群，因为如果 g_1 和 g_2 分别属于这样两个子群，则 g_1 和 g_2 同属于这两个子群中较大的一个，因而它们的乘积和逆也是如此．由于这个原因，左恩引理在群论的证明中以至一般地在抽象代数中占有重要的地位．

良序公理和左恩引理在辑逻上都等价于:

选择公理. 对于集合 S 的任何一族非空子集 $F=\{S_i\}$,存在对 F 内的子集有定义的选择函数 $f(S_i)$,它的值是 S 的元素,即有 $f(S_i)=a_i\in S_i$.

选择公理的某种表述看来要导致诡论,由于这个原因它是有可疑之处的. 当 S 是可数集时,即当它的元素可以与自然数 1, 2, 3, … 成一一对应时,这三个原理当然都成立. 对于其他集合 S,它们也有成立的,对于所有良序集合更是如此. 然而必须注意还没有人能真正构造出全体实数的一个良序来. 当在本书中利用这些原理中的一个时,应该认为"每个集合 S"的意思是"这公理在其中成立的每个集合 S".

下面是这些方法的一个有效应用:

定理 1.8.3. 设 g 是群 G 的一个元素,H 是 G 的不包含 g 的子群. 那么就存在包含 H 的一个子群 M,对不包含 g 的性质说它是极大的.

证明. 我们利用左恩引理. 包含 H 而不包含 g 的子群在包含关系下组成一个偏序集合. 它的一个全序子集中的全体子群的元素组成一个群,它也包含 H 而不包含 g. 因此就存在包含 H 而不包含 g 的一个极大子群 M.

利用这个定理,我们容易证明下列定理.

定理 1.8.4. 设 G 是一个有限生成群, H 是 G 的真子群[1]. 那么就存在 G 的包含 H 的极大真子群 M.

证明. 设 G 由 $x_1,\cdots,x_m$ 生成而且 y_1 是 $x_1,\cdots,x_m$ 中第一个不属于 H 的元素. 设 $M_1\supseteq H$,这里 M_1 对不包含 y_1 的性质说是极大的. 那么 G 的包含 M_1 作为真子集的任何子群都包含 y_1,因而 $\{M_1,y_1\}=H_1$ 也如此. 如果 $H_1=G$,则 M_1 就

1) 集合 S 的真子集是指不等于 S 的子集. ——译者

是所要的极大子群. 如果不是这样，取 $M_2 \supseteq H_1$，这里 M_2 对不包含 y_2 的性质说是极大的，这个 y_2 是 $x_1, \cdots, x_m$ 中第一个不属于 H_1 的元素. 因为 $G = \{x_1, \cdots, x_m\}$，继续这个步骤必定达到一个 $M_i \supseteq H_{i-1} \supseteq \cdots \supseteq H$，这里 $\{M_i, y_i\} = G$ 而且 $M_i = M$ 是所要的极大子群.

1.9. 群的例子

从一个集合到自身上的、保持某个性质的一一映射通常组成一个群. 很多极有趣的群都是以这一方式自然地产生的. 几何图形的对称是这一类型的. 那就是从图形到自身上的合同(即保持距离的)映射. 下面例子中的前两个是由对称组成的群.

例 1. 二面体群. $n \geqq 3$ 边的正多边形的对称组成一个 $2n$ 阶群. 它们完全由从顶点集合到自身上的映射决定. 设顶点以顺时针方向编号为 $1, 2, \cdots, n$. 顶点 1 可以映成任何顶点 $1, 2, \cdots, n$，然后其余的顶点就得以顺时针或反时针方向排列. 全体对称由旋转

$$a = \begin{pmatrix} 1, & 2, & 3, & \cdots, & n-1, & n \\ 2, & 3, & 4, & \cdots, & n, & 1 \end{pmatrix}$$

和反射

$$b = \begin{pmatrix} 1, & 2, & 3, & \cdots, & n-1, & n \\ 1, & n, & n-1, & \cdots, & 3, & 2 \end{pmatrix}$$

生成. 这时 $a^n = 1$, $b^2 = 1$, $ba = a^{-1}b$. 此外，这些关系完全决定这个群，因为由 a 和 b 生成的每个元素不外乎 $a^{i_1}b^{j_1}\cdots a^{i_r}b^{j_r}$，而由于 $ba^i = a^{-i}b$ (这可以从最后一个关系得出)，每个元素都可以改写成 a^i 或 a^ib 的形式，这里 $i = 0, 1, \cdots, n-1$; 这些就是已知群的 $2n$ 个不同的元素. 当 $n = 2$ 时，这些关系

也定义一个群，它的阶是 4．这个群叫做**四元群**.

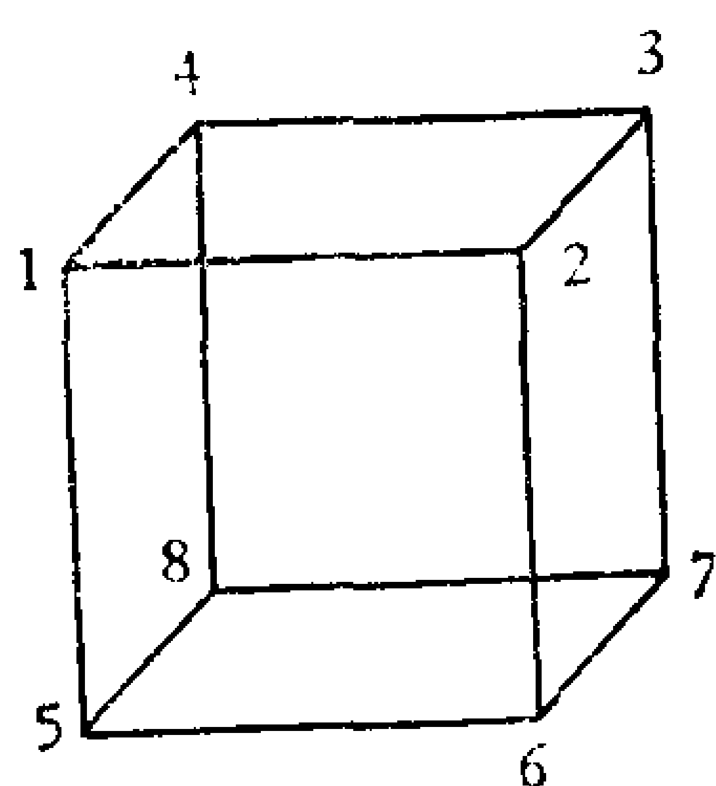


图 1　立方体的对称

例 2. 立方体的对称. 立方体的对称是由八个顶点到自身上的映射决定的．设这些顶点像图上所画的那样地编了号．对称包括了旋转

$$a=\begin{pmatrix}1,&2,&3,&4,&5,&6,&7,&8\\2,&3,&4,&1,&6,&7,&8,&5\end{pmatrix},$$

$$b=\begin{pmatrix}1,&2,&3,&4,&5,&6,&7,&8\\1,&4,&8,&5,&2,&3,&7,&6\end{pmatrix},$$

和反射

$$c=\begin{pmatrix}1,&2,&3,&4,&5,&6,&7,&8\\5,&6,&7,&8,&1,&2,&3,&4\end{pmatrix}.$$

元素 a 和 b 生成一个群 G_1，它能把每个顶点映成每个另外的顶点．这可以从下面的图表得出：

$$1\xrightarrow{a}2\xrightarrow{a}3\xrightarrow{a}4\xrightarrow{b}5\xrightarrow{a}6\xrightarrow{a}7\xrightarrow{a}8\xrightarrow{a}5\xrightarrow{b}2\xrightarrow{a^{-1}}1.$$

在这个图表里，$i\xrightarrow{x}j$ 是说元素 x 把 i 映成 j．例如 ba^2 把 4 变成 7．保持 1 不变的元素组成一个子群 H_1，而且我们可以写出

$$G_1=H_1+H_1x_2+H_1x_3+H_1x_4+H_1x_5+H_1x_6+H_1x_7+H_1x_8,$$

这里 x_i 是把 1 变成 i 的一个元素．我们不妨这样来取这些 x：$x_2=a$，$x_3=a^2$，$x_4=a^3$，$x_5=a^3b$，$x_6=a^3ba$，$x_7=a^3ba^2$，$x_8=a^3ba^3$．因为一共只有八个数字而且同一个傍系 H_1x_i 的全体元素都把 1 变成同一个 i，这就包括了 H_1 的全体可能的傍系，因而 H_1 在 G_1 内的指数是8.

立方体的保持顶点 1 不变的旋转必须使它的三个邻接的顶点作循环置换．因此 H_1 只包含 1，b，b^2，即它的阶是 3，因而 G_1 的阶是 24．反射 c 不在 G_1 内，但是由于 $c^2=1$，$ca=$

ac 和 $cb = a^2ba^2c$，因而由 a, b, c 生成的群 G 满足 $G = G_1 + G_1c$，这说明它的阶是 48. G 是立方体的全体对称的群.

例 3. 由只服从下列关系的元素 a 和 b 生成的群 G 是几阶的

$$a^7 = 1,\ b^3 = 1,\ ba = a^rb?$$

G 的每个元素可以表成 a 和 b 的一个有限序列. 根据关系 $ba = a^rb$，我们可以最终地把任何元素表成在 b 之后没有 a 的形状. 因此每个元素可以表成

$$g = a^ib^j,\ i = 0, 1, \cdots, 6;\ j = 0, 1, 2.$$

由此得出 G 的阶最多是 21. 但是真正的阶依赖于关系 $ba = a^rb$ 里的 r 的值. 我们有 $ba^2 = a^rba = a^r(a^rb) = a^{2r}b$，同理 $ba^i = a^{ir}b$. 因而 $b^2a = ba^rb = a^{r^2}b^2$. 由此得出 $b^2a^i = a^{ir^2}b^2$. 于是 $b^3a = ba^{r^2}b^2 = a^{r^3}b^3$. 但是由于 $b^3 = 1$，这给出 $a = a^{r^3}$；然而还有 $a^7 = 1$. 在值 $r = 1, 2, 3, 4, 5, 6$ 中我们发现 $r = 3, 5, 6$ 导出 $a = 1$，这时已知群只不过是由 $b^3 = 1$ 给出的 3 阶循环群. 但是 $r = 1, 2, 4$ 并不导出这个结论. 如果 $r=1$，则 $ab = ba = c$ 是一个 21 阶的元素. 反之，在 21 阶的循环群里，设 $c^{21} = 1$，只要令 $b = c^7$, $a = c^{-6}$，我们就有 $a^7 = 1$, $b^3 = 1$, $ba = ab = c$. 在 $r = 2$ 时可以取下列置换:

$$a = \begin{pmatrix} 1, 2, 3, 4, 5, 6, 7 \\ 2, 3, 4, 5, 6, 7, 1 \end{pmatrix},$$

$$b = \begin{pmatrix} 1, 2, 3, 4, 5, 6, 7 \\ 1, 5, 2, 6, 3, 7, 4 \end{pmatrix}.$$

在 $r = 4$ 时取同一置换作为 a 而取第二个置换的逆作为 b. 这个例子说明在定义关系里作很小的改变就能造成所定义的群的很大的不同.

例 4. 我们来求七个字母 A, B, C, D, E, F, G 的这样的置换群，它们使下表中的各列字母彼此置换，这时并不考

虑同一列中字母的次序:

$$A, B, C, D, E, F, G$$
$$B, C, D, E, F, G, A$$
$$D, E, F, G, A, B, C.$$

容易发现置换

$$a = \begin{pmatrix} A, & B, & C, & D, & E, & F, & G \\ B, & C, & D, & E, & F, & G, & A \end{pmatrix}$$

使各列循环地置换. 因此,如果 G_0[1] 是全体所说置换的群, H 是把第一列映成自身的置换所成的子群, 则傍系 $Ha^i(i = 1, \cdots, 6)$ 由全体把第一列映成第 $i+1$ 列的元素组成. 因此

$$G_0 = H + \cdots + Ha^6, [G_0: H] = 7.$$

在 H 内可能有元素循环地置换 A, B, D. 只要试一下就能发现这还不能决定其余的字母如何变换, 但是如果再假定 C 变成自己,则就能完全地决定一个置换

$$b = \begin{pmatrix} A, & B, & C, & D, & E, & F, & G \\ B, & D, & C, & A, & F, & G, & E \end{pmatrix}.$$

因此, 如果 K 是由保持第一列和字母 A 不变的置换所成的子群,则

$$H = K + Kb + Kb^2, \ b^3 = 1, \ [H: K] = 3.$$

在 K 内我们选出使 B 和 D 交换的一个元素. 取

$$c = \begin{pmatrix} A, & B, & C, & D, & E, & F, & G \\ A, & D, & C, & B, & F, & E, & G \end{pmatrix}.$$

于是,如果 T 是保持 A, B 和 D 都不变的子群, 则

$$K = T + Tc, \ c^2 = 1, \ [K:T] = 2.$$

在 T 内, 字母 A, B, D 不变, 字母 C 可以变成 C, E, F, G 四者中的一个. 每一种选择都恰好导出一个置换:

---

1) 原文是 G,为避免与被置换的列中的字母 G 相混而改成 G_0.——译者

$$\begin{pmatrix} A, & B, & C, & D, & E, & F, & G \\ A, & B, & C, & D, & E, & F, & G \end{pmatrix},$$

$$\begin{pmatrix} A, & B, & C, & D, & E, & F, & G \\ A, & B, & E, & D, & C, & G, & F \end{pmatrix},$$

$$\begin{pmatrix} A, & B, & C, & D, & E, & F, & G \\ A, & B, & F, & D, & G, & C, & E \end{pmatrix},$$

$$\begin{pmatrix} A, & B, & C, & D, & E, & F, & G \\ A, & B, & G, & D, & F, & E, & C \end{pmatrix}.$$

因此T是 4 阶群,K是 8 阶群,H是24阶群, G_0 是 168 阶群. 如果把七个字母 $A, \cdots, G$ 看作点，把每一列看作线，则所给的表表示具有七个点的有限射影平面，而群 G_0 正是它的直射群.

例 5. 四元数群. 以下的 8 阶群是具有很多特点的群. 它的不寻常的性质将在 §12.5 里讨论. 这里我们关心的只是用乘法表或凯雷表来表示它. 在左端记着x_i的一行和顶端记着 x_j 的一列的交叉处记着乘积 $x_k = x_i x_j$.

	x_1,	x_2,	x_3,	x_4,	x_5,	x_6,	x_7,	x_8
x_1	x_1,	x_2,	x_3,	x_4,	x_5,	x_6,	x_7,	x_8
x_2	x_2,	x_5,	x_4,	x_7,	x_6,	x_1,	x_8,	x_3
x_3	x_3,	x_8,	x_5,	x_2,	x_7,	x_4,	x_1,	x_6
x_4	x_4,	x_3,	x_6,	x_5,	x_8,	x_7,	x_2,	x_1
x_5	x_5,	x_6,	x_7,	x_8,	x_1,	x_2,	x_3,	x_4
x_6	x_6,	x_1,	x_8,	x_3,	x_2,	x_5,	x_4,	x_7
x_7	x_7,	x_4,	x_1,	x_6,	x_3,	x_8,	x_5,	x_2
x_8	x_8,	x_7,	x_2,	x_1,	x_4,	x_3,	x_6,	x_5.

在这个表里,由于每个x_i在每一行和每一列里恰好出现一次, 所以在乘积 $ab = c$ 里, a, b, c 中的任何两个都唯一决定第

三个．因此上面的表是一个拟群的乘法表．根据观察我们还看出在任何情况下都有 $x_1x_i = x_ix_1 = x_i$，因而 $x_1 = 1$ 是双边的单位元素，即这个表决定一个络．但是即使把最后两行换成

$$\begin{array}{c|cccccccc} x_7 & x_7, & x_4, & x_2, & x_1, & x_3, & x_8, & x_6, & x_5 \\ x_8 & x_8, & x_7, & x_1, & x_6, & x_4, & x_3, & x_5, & x_2 \end{array},$$

这些性质仍然保持．我们要求这个表是一个群的乘法表，为此还必须对于乘积验证结合律 $(ab)c = a(bc)$．

要完全地验证结合律在这时要作 $8^3 = 512$ 次验算．即使去掉当 a, b 或 c 有一个是单位元素时容易得出 $(ab)c = a(bc)$，也还需要 343 步验算．这里我们利用凯雷定理 1.4.2 的逆．

定理 1.9.1（凯雷定理的逆）．右正则映射 $x \to xg$ 组成群的络是群．

证明．这时在 $R(g)R(h)$ 下我们有 $1 \to g \to gh$．但是在 $R(gh)$ 下我们也有 $1 \to gh$，而且这是把 1 变成 gh 的唯一映射．因此 $R(g)R(h) = R(gh)$，因而对于每个 x，$(xg)h = x(gh)$，于是结合律成立．

在现在这个情形里我们记 $a = x_2$，$b = x_3$，并计算

$$A = R(a) = \begin{pmatrix} x_1, & x_2, & x_3, & x_4, & x_5, & x_6, & x_7, & x_8 \\ x_2, & x_5, & x_8, & x_3, & x_6, & x_1, & x_4, & x_7 \end{pmatrix},$$

$$B = R(b) = \begin{pmatrix} x_1, & x_2, & x_3, & x_4, & x_5, & x_6, & x_7, & x_8 \\ x_3, & x_4, & x_5, & x_6, & x_7, & x_8, & x_1, & x_2 \end{pmatrix}.$$

这时 $A^4 = B^4 = 1$，$A^2 = B^2$，$BA = A^3B$，我们容易证明它们生成一个 8 阶群，它正是已知络的右正则表示，因此这个络是群．上述置换的第二行是乘法表中的列．用生成元素 a 和 b 来表出时，我们有 $x_1 = 1$，$x_2 = a$，$x_3 = b$，$x_4 = ab$，$x_5 = a^2 = b^2$，$x_6 = a^3$，$x_7 = b^3 = a^2b$，$x_8 = a^3b$；再有，$a^4 = 1$，$b^4 = 1$，$b^2 = a^2$，$ba = a^3b$．

习　　题

1. 证明，从结合律 $(ab)c = a(bc)$ 得出：在 $a_1a_2\cdots a_n$ 中不改变因子次序而任意加括弧，所有得到的乘积是相同的.
2. 在任意群内证明 $(ab)^{-1} = b^{-1}a^{-1}$，更一般地有 $(a_1a_2\cdots a_{n-1}a_n)^{-1} = a_n^{-1}a_{n-1}^{-1}\cdots a_2^{-1}a_1^{-1}$.
3. 证明 a 和 a^{-1} 是同阶的.
4. 证明 ab 和 ba 是同阶的.（提示：ab 和 ba 是共轭元素.）
5. 如果 $a^m = 1$ 和 $b^n = 1$，这里 m 和 n 是正整数，又如果 $ba = ab$，证明 $(ab)^k = 1$，这里 k 是 m 和 n 的最小公倍数. 找出 $ba \neq ab$ 的一个例子，使这结果不成立.
6. 如果群 G 只有一个 2 阶元素 a，证明对于 G 的每个 x，$xa = ax$.
7. 证明，只有二阶群是恰好具有两个共轭元素类的有限群.
8. 如果 $p < q$ 是素数，证明 pq 阶群不能有两个不同的 q 阶子群.
9. 如果 H 是有限群 G 的真子群，证明 H 的所有共轭者不会包含 G 的全部元素.
10. 证明 1，2，3，4 阶的络是群，并找出一个不是群的 5 阶的络.
11. 证明，二重傍系 HxK 包含着 K 的那种右傍系，它们至少与 Hx 有一个公共元素.
12. 斯可脱 [William Scott]. 给了具有二元乘积和对所有 a 都有 $1a = a1 = a$ 的单位元素 1 的体系，证明：如果把 $a_1a_2\cdots a_n$ 的某两种不同的加括弧得出相同的值作为假设，则这个体系满足结合律.
13. 根据群的第一个定义的公理，证明单位元素 1 和逆 a^{-1} 的唯一性.
14. 如果 A 和 B 是群 G 的两个有限子群，证明子集 AB 恰好包含 $[A:1][B:1]/[A\cap B:1]$ 个不同的元素.

第二章　正规子群和同态

2.1. 正规子群

群 G 的子群 H 叫做正规子群，假如对于所有 $x\in G$，都有 $x^{-1}Hx=H$. 使用 §1.6 的术语，群 G 的子群 H 在 $N_G(H)=G$ 时是正规子群.

引理 2.1.1. G 的子群 H 是 G 的正规子群，必要而且只要每个左傍系 Hx 同时也是一个右傍系 xH.

证明. 如果对于所有 x 都有 $x^{-1}Hx=H$，则 $Hx=xH$. 反之，如果 $Hx=yH$，则 $x\in yH$，因而 $yH=xH$. 于是对于所有 $x\in G$ 都有 $Hx=xH$，因而 $x^{-1}Hx=H$.

推论 2.1.2. 指数为 2 的子群必定是正规子群.

因为如果 $G=H+Hx$，则 $G=H+xH$.

对于有限群，从 $x^{-1}Hx\subseteq H$ 得出 $x^{-1}Hx=H$. 因为 $x^{-1}Hx$ 和 H 包含同样个数的元素. 但是对于无限群却不能从包含式得出等式. 然而如果 $x^{-1}Hx\subseteq H$ 和 $xHx^{-1}\subseteq H$，则 $H=x(x^{-1}Hx)x^{-1}\subseteq xHx^{-1}\subseteq H$，因而 $H=xHx^{-1}$，同理 $H=x^{-1}Hx$. 因此 $x^{-1}Hx\subseteq H$ 对于所有 x 都成立是 H 正规的充分条件.

没有正规真子群的群叫做单纯群. “单纯”这个词必须当作专门词来理解. 根据定理 1.5.4，没有任何真子群的群是素数阶的有限循环群，这些群不论就专用词说，还是就更普通的（即不复杂的）意义说，都是单纯的. 但是还有很多其他的单纯群，其中一个是在 §1.8 的第四个例子里的 168 阶群. 决定全部有限阶的单纯群是一个未解决的问题. 有人猜想除素

数阶群外，单纯有限群必定是偶数阶的，但即使这个问题也显得是一个非常难的问题.

2.2. 同态的核

假定群H是群G的同态像. 考虑G中所有映成H的单位元素的元素$t\in G$的集合T.

$$G\to H,\ T\to 1. \tag{2.2.1}$$

在§1.4里说过，$1\to 1$，因而$1\in T$. 如果$t\to 1$，$t^{-1}\to u$，则$1=tt^{-1}\to u$. 但是$1\to 1$，因而$u=1$，所以$t^{-1}\to 1$而$t^{-1}\in T$. 又如果$t_1\to 1$，$t_2\to 1$，则$t_1t_2\to 1$，因而$t_1t_2\in T$. 因此T是G的子群. 其次如果$x\in G$，$t\in T$，则$x\to y$，$t\to 1$，$x^{-1}\to y^{-1}$，而且$x^{-1}tx\to y^{-1}1y=1$，因而$x^{-1}tx\in T$，所以T是G的正规子群. T叫做同态$G\to H$的核.

定理 2.2.1（第一同态定理）. 在同态$G\to H$下，G的映成H的单位元素的元素的集合T是G的正规子群. G的两个元素在H里有相同的像，必要而且只要它们属于T的同一个傍系.

证明. 我们已经证明了T是G的正规子群. 假定$x\to u$，$y\to u$，$x,\ y\in G$，$u\in H$. 那么$xy^{-1}\to 1$而$xy^{-1}\in T$，因而$x\in Ty$，即x和y属于T的同一个傍系. 反之，如果$x\in Ty$，则$x=ty$，又如果$y\to u$，则（由于$t\to 1$）就有$x\to u$，即x和y在H内有相同的像.

2.3. 商　　群

在上一节里证明过，群G的同态核是一个正规子群T. 反之，每个正规子群T都是一个同态（事实上还是唯一的同态）

的核．假定

$$G = T + Tx_2 + \cdots + Tx_r, \qquad (2.3.1)$$

这里T是G的正规子群．我们可以取傍系 Tx_i 作为一个集合H的元素．我们定义H里的乘法为

$$(Tx_i)(Tx_j) = Tx_k, \qquad (2.3.2)$$

假如在G内 $x_ix_j \in Tx_k$.

必须证明乘积是唯一确定的．设 t_1x_i 和 t_2x_j，分别是 Tx_i 和 Tx_j 的任意元素．于是 $t_1x_it_2x_j = t_1x_it_2x_i^{-1} \cdot x_ix_j = t_3x_ix_j$，因为$T$是正规子群．而如果 $x_ix_j \in Tx_k$，则也有 $t_3x_ix_j \in Tx_k$．因而 Tx_i 中一个元素和 Tx_j 中一个元素的所有乘积是同一个傍系 Tx_k 的元素．因此（2.3.2）中的乘积只依赖于傍系而不依赖于代表元素的选取；这说明 H中的乘法有意义．

因为T是正规子群，$T^2 = T$，$Tx_i = x_iT$．因此在H内，由于 $T \cdot Tx_i = Tx_i$，$Tx_i \cdot T = Tx_iT = TTx_i = Tx_i$，$T$ 是单位元素．其次，因为 $(Tx_iTx_j)Tx_k = Tx_ix_jx_k = Tx_i(Tx_jTx_k)$，乘法满足结合律．如果 $x_i^{-1} \in Tx_j$，则 Tx_iTx_j 包含 $x_ix_i^{-1} = 1$，因而 $Tx_iTx_j = T$，于是由于同理可证 $Tx_jTx_i = T$，在H内 Tx_j 是 Tx_i 的逆．这样就证明了H是一个群，它叫做G对T的商群．我们记做 $H = G/T$．

定理 2.3.1（关于同态的第二定理）．给了群 G 和正规子群 T．那么如果 $H = G/T$，则就存在同态 $G \to H$，它的核是 T．这个同态可以由 $g \to Tx_i$ 给出，假如在G内$g \in Tx_i$.

证明．设在G内 $g \in Tx_i$，考虑从 G 到H上的映射 $g \to Tx_i$．如果 $g_1 \in Tx_i$，$g_2 \in Tx_j$，则（我们曾经证明过）$g_1g_2 \in Tx_k$，这里 $x_ix_j \in Tx_k$．因此 $g_1g_2 \to Tx_k = Tx_iTx_j$．因而从$G$到$H$上的这个映射保持了乘积，即是一个同态．因为$T$是 G/T 的单位元素，所以 $g \to 1$（在H内 $= T$），必要而且只要在G内 $g \in T$，因而T是这个同态的核．这就完成了证明．

定理 2.3.2（关于同态的第三定理）. 如果 $G \to K$ 是从 G 到 K 上的同态，T 是这个同态的核，则 K 同构于 $G/T = H$. 如果在同态 $G \to K$ 下 $x \to x^*$，则 $x^* \rightleftarrows Tx$ 是在 K 和 H 之间的同构.

证明. 因为在 T 的同一个傍系里的 G 的元素在 K 内有相同的像，对应 $x^* \rightleftarrows Tx$ 是一一的. 但是如果 $x \to x^*$，$y \to y^*$，则 $xy \to x^*y^*$. 由于 $xy \in Txy$，因而 $x^*y^* \rightleftarrows Txy = TxTy$. 因此对应 $x^* \rightleftarrows Tx$ 保持乘积，即是 K 和 $H = G/T$ 的一个同构.

让我们总结一下关于同态的这三个主要定理的内容. 我们证明了：任何同态的核是正规子群，任何正规子群是一个同态的核，这同态的像（在同构的意义下）是唯一的，并且这同态像是已知群对已知正规子群的商群.

定理 2.3.3. 如果 A 和 B 是群 G 的子群而且其中有一个是正规子群，则 $A \cup B = AB$.

证明. 我们只要证明任何有限乘积 $x_1x_2\cdots x_s$（$x_i \in A$ 或 B）都能改写成 ab 的形状. 然而如果 B 是正规的，则 $ba = aa^{-1}ba = ab'$，又如果 A 是正规的，则 $ba = bab^{-1}b = a'b$，所以我们可以改写已知乘积使得在 a 前没有 b. 这样就使已知乘积成为 $a_1a_2\cdots a_jb_{j+1}\cdots b_s = ab$，这里 $a_i, a \in A$ 而 $b_i, b \in B$.

定理 2.3.4. 设 T 是 G 的正规子群. 那么在 $H = G/T$ 的子群 K^* 和使 $G \supseteq K \supseteq T$ 的 G 的子群 K 之间存在一一对应，这里 K 由 G 中映成 K^* 的元素的全体元素组成. 如果 K^* 在 H 内是正规的，则 K 在 G 内是正规的，反之亦然. 再有 $[G:K] = [H:K^*]$.

证明. G 的子群在 H 内的像显然是子群. 现在设 K^* 是 H 的子群，则 K^* 在 G 内的逆像 K 包含着 1 的逆像 T. 逆像也满足关于子群的所有要求.

因此H的子群 K^* 的逆像是唯一的子群K使得 $G\supseteq K\supseteq T$，而且这个 K^* 是K在同态 $G\to H$ 下的唯一的像．因此 $K\rightleftarrows K^*$ 是在 $G\supseteq K\supseteq T$ 和 $H\supseteq K^*\supseteq 1$ 之间的 1—1 对应．如果K^* 在H内是正规的，则 $x^{-1}Kx\to x^{*-1}K^*x^*=K^*$，因而对于任何 x 都有 $x^{-1}Kx\subseteq K$，所以K在G内是正规的．再有，如果K是正规的，则它的像 K^* 显然也是正规的．最后，傍系 K^*g^* 的逆像是一个傍系 Kg，因而$[G:K]=[H:K^*]$．

如果任意子群A的像是 A^*，则容易得出 A^* 的逆像是 $A\cup T=AT$．

2.4. 算　子

从群G到自身的映射 $\alpha:g\to g^\alpha$ 叫做G的自同态或G上的算子，假如 $(xy)^\alpha=x^\alpha y^\alpha$．因而自同态是从$G$到自身的同态．自同构是指从$G$到自身上的 1—1 自同态．如果从 $g^\alpha=h^\alpha$ 得出 $g=h$，则自同态是同构，在有限群的情形这必定是自同构．但是一个无限群可以同构于它的真子群．例如 $x\to 2x$ 是自同态，它是从整数加法群到自身的同构，但是不是自同构．

G的子群H叫做对自同态 α_i 容许的，假如对于所有 α_i，$H^{\alpha_i}\subseteq H$．从定义直接得出，容许子群的并和交是容许子群．明显地，群的算子α也可以看作是容许子群的算子．但是可能出现这样的情况，对于整个群不同的两个算子可以在作用于一个容许子群时是相同的．再有，如果 $G\to K$ 是从G到K上的同态，它的核T是对自同态α容许的，则我们可以在K内定义一个对应的算子．我们令

$$(Tx)^\alpha=Tx^\alpha. \tag{2.4.1}$$

这是一个自然的定义，因为自同态α作用于傍系 Tx 的元素

只能得出属于 Tx^α 的元素. 我们容易验证这在 K 内决定一个算子,而且如果在同态 $G \to K$ 下 $x \to x^*$, 则$x^\alpha \to x^{*\alpha}$.

两个群A和B叫做算子同构的，假如存在群之间和它们的算子之间的 1—1 对应 $A \rightleftarrows B$ 和 $\alpha_i \rightleftarrows \beta_i$, 使得 $a \rightleftarrows b$ 是一个同构而且在这同构下 $a^{\alpha_i} \rightleftarrows b^{\beta_i}$. 因而算子同构强于同构.

定理 2.4.1. 给了群G和G上的算子集合Ω. 假定 A 是G的容许子群，T 是容许正规子群. 那么 $A \cap T$ 是A的容许正规子群，而且商群 $A \cup T/T$ 和 $A/A \cap T$ 是算子同构的.

证明. $A \cap T$ 作为Ω子群(即在Ω下容许的子群) 的交是A的Ω子群. 如果$u \in A \cap T, a \in A$, 则 $a^{-1}ua \in A$. 又因为T在G内是正规的而且 $u \in T$, 所以 $a^{-1}ua \in T$. 因此[1] $a^{-1}ua \in A \cap T$, 即 $A \cap T$ 在A内是正规的.

让我们记 $D = A \cap T$.

$$A = D + Da_2 + \cdots + Da_r. \tag{2.4.2}$$

那么我们可以断定

$$A \cup T = T + Ta_2 + \cdots + Ta_r, \tag{2.4.3}$$

这里用在 (2.4.2) 里的同一些记号来表示 (2.4.3) 里的傍系. 这时如果 $Ta_i = Ta_j$, 则 $a_ia_j^{-1} \in T$. 但是 $a_ia_j^{-1} \in A$,因而$a_ia_j^{-1} \in A \cap T = D$, 这与 (2.4.2) 矛盾. 因此 (2.4.3) 里的傍系 Ta_i 都是不同的. 其次,因为T是正规子群，$A \cup T = TA$, 所以 T在 $A \cup T$ 内的傍系都有形状 $Ta = Tda_i$, 这里从(2.4.2)得出 $a = da_i$. 但是由于 $d \in T$, $Tda_i = Ta_i$, 因而(2.4.3)中的傍系穷尽了 $A \cup T$. 对应

$$Da_i \rightleftarrows Ta_i \tag{2.4.4}$$

1) 这里原书排印有错. ——译者

是在 (2.4.2) 和 (2.4.3) 里的傍系之间的 1—1 对应，也就是 A/D 和 $A\cup T/T$ 的元素之间的 1—1 对应．又如果 $a_ia_j = da_k$，这里$d\in D$，则因为 $D\subseteq T$，我们就同时有 $Da_iDa_j = Da_k$ 和 $Ta_iTa_j = Ta_k$．因而对应 (2.4.4) 是在商群 A/D和 $A\cup T/T$ 之间的同构．算子 $\alpha\in\Omega$ 按照规则 $(Da_i)^\alpha = Da_i^\alpha$ 和 $(Ta_i)^\alpha = Ta_i^\alpha$ 决定 A/D 的一个算子和 $A\cup T/T$ 的一个算子．对于以这种方式给定的算子，立即得出 (2.4.4) 决定一个算子同构．这就完成了定理的证明．

我们容易验证：群G的子群K是正规子群，必要而且只要它在G的内自同构族下是容许的．我们用算子来给出子群的正规性的两个逐步加强的定义．在群的全体自同构下容许的子群叫做**特征子群**，在全体自同态下容许的子群叫做**完全不变子群**．于是群G的中心Z就是一个特征子群，因为如果对于所有 $g\in G$ 都有 $zg = gz$，则对于自同构 α，我们有 $z^\alpha g^\alpha = g^\alpha z^\alpha$，而当 g 通过G的全体元素时，g^α 也通过G的全体元素，因而我们得出 $z^\alpha\in Z$．但是中心不一定是完全不变子群．举例说，考虑由下列关系定义的 16 阶群 $G: a^4 = 1$，$b^2 = c^2 = 1$，$ba = a^{-1}b$，$ca = ac$，$cb = bc$．这里中心Z是 4 阶的而且由 a^2 和 c 生成．这时映射 $a\to b$，$b\to b$，$c\to b$ 决定G的一个自同态，它把属于中心的元素 c 映成 b，后者不属于中心．但是自同态保持元素的形式，因而由所有$x^3(x\in G)$或所有 $x^{-1}y^{-1}xy(x, y\in G)$ 生成的子群是完全不变的．

正规性的这两种加强的形式的一个特别有用的性质在于：虽然群G的正规子群K的正规子群H不一定是G的正规子群，但是从定义可以得出，特征子群的特征子群是特征子群，完全不变子群的完全不变子群是完全不变子群．又正规子群的特征子群是正规子群．

2.5. 直积和笛卡儿乘积

给了两个群A和B，我们可以构造有序对子(a, b)，$a \in A, b \in B$的集合．如果用下列规则定义乘积：

$$(a_1, b_1)(a_2, b_2) = (a_1a_2, b_1b_2), \tag{2.5.1}$$

则这种有序对子就组成一个新的群，它叫做直积$A \times B$．要验证相乘规则(2.5.1)满足以$(1, 1)$为单位元素的群的公理并不困难，只要依靠这些公理对于A和B的有效性．其次，对应$(a, b) \rightleftarrows (b, a)$表明$A \times B$和$B \times A$是同构的，所以我们可以不强调顺序而说两个群的乘积．对应$a \rightleftarrows (a, 1)$是在$A$和$A \times B$内第二个分量是单位元素的元素集合之间的同构．同理，对应$b \rightleftarrows (1, b)$是在$B$和由元素$(1, b)$组成的子群之间的同构．我们把$A$和$B$与这两个子群等同起来．在这个等同下我们说$G = A \times B$是它的子群$A$和$B$的直积．因为$(a, 1)(1, b) = (a, b) = (1, b)(a, 1)$，所以在$A \times B$内$A$的每个元素与$B$的每个元素都可交换；即$ab = ba$对于$a \in A, b \in B$.

在直积内，$(a, b)^{-1} = (a^{-1}, b^{-1})$．因此$(a_1, b_1)^{-1}(a_2, 1) \cdot (a_1, b_1) = (a_1^{-1}a_2a_1, 1)$，即$A$是$A \times B$的正规子群．同理$B$是$A \times B$的正规子群．同时具有形状$(a, 1)$和$(1, b)$的元素是$(1, 1)$，因而$A \cap B = 1$．其次，$A \cup B$包含所有乘积$(a, 1)(1, b) = (a, b)$，因而$A \cup B = A \times B$．在$A$和$B$之间的这些关系决定了$A \times B$.

定理 2.5.1. 群G同构于两个子群A和B的直积，必要而且只要A和B是正规子群而且$A \cap B = 1, A \cup B = G$.

证明. 我们已经知道，在直积$A \times B$内，子群A和B具有这些性质．假定反过来，A和B是G的正规子群，而且

$A\cap B=1$, $A\cup B=G$. 考虑元素 $a^{-1}b^{-1}ab=a^{-1}(b^{-1}ab)=(a^{-1}b^{-1}a)b$, 这里 $a\in A$, $b\in B$. 因为 A 和 B 是正规子群，从第一种分括它是 A 的元素，而从第二种分括它是 B 的元素. 它必须是 $A\cap B=1$ 的元素，因而 $a^{-1}b^{-1}ab=1$, 即 $ab=ba$. 根据定理 2.3.3, $G=A\cup B=AB$, 因而每个元素 g 可以写成 $g=ab$. 其次，这种写法是唯一的，因为从 $a_1b_1=a_2b_2$ 得出 $a_2^{-1}a_1=b_2b_1^{-1}\in A\cap B=1$, 因而 $a_1=a_2$, $b_1=b_2$. 现在当 $g=ab$ 时，我们令 $g\rightleftarrows(a,b)$. 如果 $g_1=a_1b_1$, $g_2=a_2b_2$, 则 $g_1g_2=a_1b_1a_2b_2=(a_1a_2)(b_1b_2)$. 因此在 G 和 $A\times B$ 之间的这个对应不仅是一一的，而且还保持了乘积，因而我们确立了 G 和 $A\times B$ 之间的一个同构.

我们可以推广前面的概念而定义任意有限个或无限个群的乘积. 假定给了一组群 A_i, 这里 i 遍历某个指标集 I (在某些定理里我们假定 I 是良序的). 我们构造**形式乘积** $\prod_{i\in I}a_i$. 形式乘积只不过是从每个群 A_i 选取一个元素 a_i 罢了. 全体形式乘积组成的群叫做这些 A_i 的笛卡儿乘积，这时相乘法则是:

$$\prod_{i\in I}a_i\cdot\prod_{i\in I}b_i=\prod_{i\in I}c_i, \tag{2.5.2}$$

这里对于每个 $i\in I$ 都有 $c_i=a_ib_i$.

在笛卡儿乘积中，由除有限个指标外都有 $a_i=1$ 的元素组成的子群叫做 A_i 的**直积**. 明显地，当因子的个数有限时，直积就是笛卡儿乘积. 在两种乘积中，对于 $i\neq j$ 有 $a_i=1$ 的元素 $\prod_i a_i$ 组成一个正规子群，它同构于 A_j. 如果把 A_j 与这个子群等同起来，则我们有 $A_j\cap\left(\bigcup_{i\neq j}A_i\right)=1$. 这里 $\bigcup_{i\in I}A_i$ 表示直积.

定理 2.5.2. 群G同构于子群$A_i(i\in I)$的直积，假如:

1) 每个A_i是正规子群.

2) $A_j\cap\left(\bigcup_{i\neq j}A_i\right)=1$ 对于每个$j\in I$.

3) $G=\bigcup_{i\in I}A_i$.

证明. 这个定理的证明很接近于定理 2.5.1 的证明. 根据 1) 和 2)，每个a_j都与$i\neq j$的a_i的任何有限乘积可交换. 又根据 1)，2) 和 3)，每个$g\in G$都可以表成A_i的元素的有限乘积，而且如果不考虑顺序，把它表成从每个A_i最多只取一个元素的乘积时只有唯一的表达式. 这就给出在G和A_i的直积之间的一个同构. G的元素可以表成$g=1$或$g=b_1\cdots b_m$，$b_k\neq 1$，$k=1,\cdots,m$，这些b是从不同的A_i取出的，于是g对应于元素$\prod_{i\in I}a_i$，这里在g的乘积形式中有$b_k\in A_i$时取$a_i=b_k$，否则取$a_i=1$. 这个对应产生在G和A_i的直积之间的一个同构.

习　题

1. 证明 2 阶群是每一个二面体群的同态像.
2. 证明，如果$p<q$都是素数，则在pq阶群中存在q阶的正规子群. （参看第一章的习题 8. ）
3. 证明四元数群的子群都是正规的.
4. 在立方体内，设x，y，z是连结对面中点的三条线. 证明立方体的对称群G对这些线的作用是一个 6 阶的置换群H. 证明H是G的一个同态像.
5. 考虑从实数集合到自身上的 1—1 映射$x\rightleftarrows ax+b$，这里a，b都是实数，$a\neq 0$. 证明这些映射组成一个群G，在其中平移$T:x\rightleftarrows x+t$组成一个正规子群. 问商群G/T是什么?
6. 对于群G的每个元素b，定义一个共轭算子b: $g\rightarrow g^b=b^{-1}gb$. 对全体这种算子来说，什么子群是容许的? 如果$T$是$G$的正规子群，证明在$H=G/T$里导出的算子也是共轭算子.

第三章　阿贝尔群初步

3.1. 阿贝尔群的定义．循环群

群G在满足交换律时：

$$G4,\ ba = ab,\ 对于所有\ a,\ b \in G$$

叫做阿贝尔群．当 $ab = ba$ 时我们也说元素 a 和 b 可交换．

在 § 1.5 里我们定义循环群为由单独一个元素 b 生成的群，它的全体元素都是 b 的方幂．因为对于任何整数 i 和 j 都有 $b^ib^j = b^jb^i = b^{i+j}$，所以循环群都是阿贝尔群．在 § 1.5 里还说过，在同构的意义下只有唯一的无限阶循环群和对于每个正整数 n 的唯一的 n 阶循环群．又循环群的每个子群也是循环群．让我们来证明这一点．

定理 3.1.1. 无限循环群的每一个不是单位元素群的子群是有限指数的无限循环群，而且对于每个有限指数存在唯一的子群．n 阶的有限循环群的每个子群是阶能整除 n 的循环群，而且对于每个能整除 n 的阶，存在唯一的子群．

证明．给定由元素 b 生成的循环群G和它的子群H．如果H不是单位元素群而且 $b^i \in H$，则 $b^{-i} \in H$，而且方次数 i 和 $-i$ 中有一个是正的．假定m是H中元素的最小的正的方次数，而且设 b^t 是H的任何元素．那么，适当选取 r，我们有 $t = mr + s,\ 0 \leqslant s < m$．于是 $b^t = (b^m)^rb^s$．因为b^t 和 b^m都属于H，所以 b^s 也属于H．但是如果 s 是 $0 \leqslant s < m$ 中不是 0 的数，这就将与m是H中元素的 b 的最小正方次数相矛盾．因此 $s = 0$，而且 $b^t = (b^m)^r$，因而H的全体元素都是 b^m 的

方幂，即H是循环群．因为对于任何整数x，我们有$x=km+i$，这里i是$0, 1, \cdots, m-1$中的一个，所以我们容易验证

$$G = H + Hb + \cdots + Hb^{m-1}. \tag{3.1.1}$$

方程（3.1.1）包含了H的全体可能的傍系而且它们是互不相同的，因为如果在从0到$m-1$的范围里取$i \neq j$而且$b^i = hb^j$，则就将得出在H内有b的更小的正的方幂，它就是b^{i-j}或b^{j-i}．因此$[G: H] = m$．这时m是包含在H中的b的最小正方次数而且也是H在G内的指数．于是，如果G是无限的，则由于对任意整数m，元素$(b^m)^r$组成一个子群，所以存在指数m的唯一子群．如果G是n阶的有限群，则$b^n = 1$，因而$n = mr$，即m是n的约数．这时对于整除n的每个m，如果$n = mr$，则元素$1, b^m, b^{2m}, \cdots, b^{(r-1)m}$组成一个子群，它的阶是$r$，指数是$m$．因为$n = mr$可以是把$n$分成两个因子的任何因子分解，所以对于整除$n$的每个阶$r$，存在唯一的子群．

3.2. 关于阿贝尔群构造的若干定理

无限阿贝尔群可以有很复杂的构造．举一个简单的例子，零以外的全体复数的乘法群有无限阶的元素而且还有任意有限阶的元素．

如果在一个阿贝尔群里，$a^n = 1$和$b^m=1$，则$(a^{-1})^n=1$和$(ab)^{mn} = 1$，因而在任何阿贝尔群A里，所有有限阶的元素组成一个子群F．A的每个自同态α把有限阶元素映成有限阶元素．因此在§2.4的意义下，F是A的完全不变子群．在§1.8里我们把全体元素都是有限阶的群叫做**周期群**（在群论的某些应用里也有叫做**挠群**的）．相反地，除单位元素外没有有限阶元素的群叫做**无周期群**（或**不挠群**）．

定理 3.2.1. 给了阿贝尔群 A. 设 F 是有限阶元素的子群. 那么 A/F 是无周期的.

证明. 假定相反地在 A/F 里有 $x \neq 1$ 具有有限的阶 m. 又在同态 $A \to A/F$ 下设 $u \to x$. 那么 $u^m \to x^m = 1$, 因而 $u^m \in F$, 即 u^m 是有限阶的, 设它的阶是 n. 于是 $(u^m)^n = 1$, 因而 u 本身是有限阶的. 因此 $u \in F$ 而 $u \to 1$, 然而我们曾假定 $x \neq 1$.

这个定理使得构造全体阿贝尔群的问题简化成三个比较简洁的问题:

1) 决定全体周期阿贝尔群.

2) 决定全体无周期阿贝尔群.

3) 构造一个阿贝尔群 A, 它以已知周期群 F 作为子群, 使得商群 A/F 同构于已知无周期群 H. 这三个问题中还没有一个完全解决, 但在现在我们对第一个问题知道得最多而对第三个问题知道得最少.

在阿贝尔群 A 内, 一组元素 a_i 叫做无关的, 假如只有在对于每个 i 都有 $a_i^{e_i} = 1$ 时, 才有有限乘积 $\prod_i a_i^{e_i} = 1$. 如果 a_i 是无关的而且生成 A, 则就说 a_i 组成 A 的一个基底. 因此元素 a_i 组成 A 的基底, 必要而且只要 A 是由 a_i 生成的循环群的直积.

假定阿贝尔群 A 由元素 $a_1, \cdots, a_r$ 生成. 那么 A 的每个元素都可以表成 $a_1^{u_1} \cdots a_r^{u_r}$, 这里 u_i 都是整数. 如果

$$a_1^{x_1} \cdots a_r^{x_r} = 1 \tag{3.2.1}$$

是关于这些生成元素的一个关系, 则我们说

$$a_1^{-x_1} \cdots a_r^{-x_r} = 1 \tag{3.2.2}$$

是它的逆关系. 从 A 内成立的关系集合 S, 取 S 的关系和 S 的关系的逆的乘积可以导出别的关系. 两个关系集合 S_1 和 S_2

叫做等价的，假如每个集合的关系都能以这种方式从另一集合的关系导出．容易看出这是一种真正的等价关系．一个关系集合 S 叫做 A 的定义关系集合，假如在 A 内成立的每个关系都能从 S 的关系导出．可以证明关于生成元素 $a_1, \cdots, a_r$ 的关系的任意集合 S 是由 $a_1, \cdots, a_r$ 生成的阿贝尔群 A 的定义关系集合，在其中从 S 导出的关系成立，而没有其他的关系成立。当然群 A 可以简化到只有单独一个单位元素．

定理 3.2.2. 由有限的 r 个元素生成的阿贝尔群具有不超过 r 个元素组成的一个基底．

证明． $r=1$ 时定理显然成立，因为这时 A 是循环群．假定 A 由 $a_1, \cdots, a_r$ 生成． 我们对 r 以及在固定了 r 时对在关系

$$a_1^{x_1}\cdots a_r^{x_r}=1 \tag{3.2.3}$$

里使 $x_i=m$ 的最小正整数 m 施行归纳法． 如果只有全体 $x_i=0$ 的唯一关系，则 A 是无限循环群 $\{a_i\}$ 的直积，因而定理成立．否则某个关系或它的逆将包含有正的方次数．在必要时把 a 重新编号，总可以假定在一个关系里的最小正的方次数是 $x_1=m$．如果 $m=1$，则我们有

$$a_1=a_2^{-x_2}\cdots a_r^{-x_r}, \tag{3.2.4}$$

因而 A 就由 $r-1$ 个元素 $a_2, \cdots, a_r$ 生成，于是根据归纳假设，定理成立．现在假定在下列关系里 $x_1=m>1$：

$$a_1^m a_2^{x_2}\cdots a_r^{x_r}=1. \tag{3.2.5}$$

设 $y_1, \cdots, y_r$ 是其他一个关系里的方次数．那么对于任何整数 k，从这个关系和 (3.2.5) 可以导出一个关系具有方次数 y_1-km, y_2-kx_2, $\cdots$, y_r-kx_r． 我们可以选取 k 使得 $0\leqslant y_1-km<m$． 但是因为 m 是在所有关系里的最小正的方次数，我们必须有 $y_1-km=0$，因而具有方次数 $y_1, \cdots, y_r$ 的关系可以由 (3.2.5) 和具有方次数 0, y_2-kx_2, $\cdots$, y_r-kx_r

的关系导出．因此A的全体关系的集合等价于由（3.2.5）和只包含a_2, $\cdots$, a_r的关系组成的集合 S.

在(3.2.5)里设$x_2 = k_2m + s_2, \cdots, x_r = k_rm + s_r$，这里我们取$k_i$, $i = 2, \cdots, r$，使得 $0 \leqslant s_i < m$. 如果我们取一个新的元素

$$a_1^* = a_1a_2^{k_2}\cdots a_r^{k_r}, \tag{3.2.6}$$

则 $a_1^*, a_2, \cdots, a_r$ 也生成A，而以这些生成元素表出时，(3.2.5)变成

$$a_1^{*m}a_2^{s_2}\cdots a_r^{s_r} = 1. \tag{3.2.7}$$

这时如果有某个 s 不是零，则它是小于m的正数，因而可以运用归纳假设．而如果 $s_2 = \cdots = s_r = 0$，则(3.2.7)变成

$$a_1^{*m} = 1. \tag{3.2.8}$$

于是因为(3.2.5)和只包含a_2, $\cdots$, a_r的关系组成 A 的以生成元素a_1, a_2, $\cdots$, a_r表出的定义关系集合，所以(3.2.8)和只包含a_2, $\cdots$, a_r的关系组成A的以生成元素 $a_1^*, a_2, \cdots, a_r$表出的定义关系集合．因此A是由 a_1^* 生成的m阶循环群和由$r-1$个元素a_2, $\cdots$, a_r生成的群的直积，而根据归纳假设，后者是不多于$r-1$个循环群的直积．这样我们就在所有的情况下证明了定理．

为了探讨周期阿贝尔群，我们用到在任何群里都成立的一个引理．

引理 3.2.1. 设x是在任何群里的一个 mn 阶元素，这里m和n是互素的整数．那么x可以唯一地表成$x = yz = zy$，这里y的阶是m，z的阶是 n. y 和z都是x的方幂

证明. 我们用（a, b）表示两个整数a和b的最大公约数．于是 m 和n互素就可以表成$(m, n) = 1$. 根据欧几里得算法，存在整数u和v，使得$um + vn = 1$，因而$x = x^{vn} \cdot x^{um} = x^{um}x^{vn}$. 令$y = x^{vn}$, $z = x^{um}$. 于是$x = yz = zy$而且

$y^m = x^{vnm} = 1$ 和 $z^n = x^{umn} = 1$. 因此 y 的阶是 m 的约数 m_1, z 的阶是 n 的约数 n_1. 但是从 $x = yz = zy$ 得出 x 的阶是 m_1n_1 的约数. 而因为 x 的阶是 mn, 所以由此得出 $m_1 = m$ 是 y 的阶, $n_1 = n$ 是 z 的阶. 设 x 另有一个表达式 $x = y_1z_1 = z_1y_1$, 这里 y_1 是 m 阶的, z_1 是 n 阶的. 我们首先注意到 y_1 和 z_1 都与 x 可交换,这是因为 $xy_1 = y_1z_1y_1 = y_1x$ 和 $xz_1 = z_1y_1z_1 = z_1x$. 于是因为 y 和 z 都是 x 的方幂. 它们也与 y_1 和 z_1 可交换. 现在从 $yz = x = y_1z_1$ 引出一个元素 $w = y_1^{-1}y = zz_1^{-1}$. 然而 y 和 y_1 是 m 阶的可交换的元素, z 和 z_1 是 n 阶的可交换的元素. 因此元素 w 同时满足 $w^m = 1$ 和 $w^n = 1$, 于是因为 $(m, n) = 1$, 这就导出 $w = 1$. 因而 $y_1 = y$, $z_1 = z$,这就证明了表达式的唯一性.

重复应用这个引理, 我们得出:

引理 3.2.2. 设 x 是 $n = n_1n_2\cdots n_r$ 阶的元素, 这里当 $i \neq j$ 时, $(n_i, n_j) = 1$. 那么 x 有唯一的表达式 $x = x_1x_2\cdots x_r$, 这里 $x_jx_i = x_ix_j$ 而且 x_i 的阶是 n_i. 每一个 x_i 都是 x 的方幂.

特别地, 如果 $n = p_1^{e_1}\cdots p_r^{e_r}$, 这里 $p_1, \cdots, p_r$ 是互不相同的素数, 则我们可以取 $n_i = p_i^{e_i}$ 而运用这个引理.

在周期阿贝尔群 A 内考虑阶为固定素数 p 的方幂的元素的集合 P, 这时我们把单位元素看作阶为 $p^0 = 1$ 而包括在内. 如果 $x^{p^a} = 1$, $y^{p^b} = 1$, 则 $(xy)^{p^c} = 1$, 这里 $c = \max(a, b)$, 而且 $(x^{-1})^{p^a} = 1$. 因此 P 是一个子群, 它叫做**西罗 p 子群** $S(p)$. 我们也把 P 叫做阿贝尔 p 群.

定理 3.2.3. 周期阿贝尔群是它的西罗子群 $S(p)$ 的直积.

证明. 明显地, A 的西罗子群的直积 $\prod_p S(p)$ 是 A 的子群. 但是根据引理 3.2.2, 如果 $x \in A$ 的阶是 $n = p_1^{e_1}\cdots p_r^{e_r}$, 则

$x = x_1x_2\cdots x_r$，这里 $x_i \in S(p_i)$；所以 A 的每个元素 x 属于西罗子群的直积，因而这个直积必须是整个群 A.

3.3. 有限阿贝尔群. 不变量

有限阿贝尔群当然是周期的和有限生成的. 应用上一节中的结果，我们可以提出以下的定理：

定理 3.3.1. 阶为 $n = p_1^{e_1}\cdots p_r^{e_r}$ 的有限阿贝尔群是西罗子群 $S(p_1), \cdots, S(p_r)$ 的直积. 这时 $S(p_i)$ 是 $p_i^{e_i}$ 阶的而且是阶为 $p_i^{e_{i1}}, \cdots, p_i^{e_{is}}$（这里 $e_{i1} + \cdots + e_{is} = e_i$）的循环群的直积.

证明. 在 n 阶阿贝尔群里，元素的阶是 n 的约数，因而对应于不整除 n 的素数的西罗子群只能包含单位元素. 因此，如果 $p_1, \cdots, p_r$ 是整除 n 的不同的素数，则已知群就是一个直积 $S(p_1) \times \cdots \times S(p_r)$. 但是这并没有指出 $S(p_i)$ 的阶，也许这些群中有一些是单位元素群. 因为 $S(p_i)$ 是单位元素群或者阶为 $p_i^{e_{i1}}, \cdots, p_i^{e_{is}}$ 的循环群的直积，所以 $S(p_i)$ 的阶是这些阶的乘积（设 $S(p_i)$ 的阶是 $p_i^{t_i}$，于是 $t_i = e_{i1} + \cdots + e_{is}$），而且整个群的阶是这些 $S(p_i)$ 的阶的乘积. 但是因为整数 n 的因子分解是唯一的，所以对于每个 i 都有 $p_i^{t_i} = p_i^{e_i}$. 作为这个定理和定理 3.1.1 的结果，我们有下面的推论.

推论 3.3.1. 如果 p 是整除 n 的素数，则 n 阶的阿贝尔群总含有 p 阶的元素.

一个有限的阿贝尔 p 群 $A(p)$ 常常可以以几种方式表成循环群的直积. 举例说，设 $a^8 = 1$，$b^4 = 1$，那么群 $A(2) = \{a\} \times \{b\}$ 是 32 阶的. 如果我们取 $c = ab$ 和 $d = a^4b$，则 $c^8 = 1$，$d^4 = 1$，$a = c^5d^{-1}$，$b = c^4d$. 我们容易验证 $A(2) = \{c\} \times \{d\}$. 在这个情形里，$A(2)$以两种不同的方式成为循环

群的直积，但是因子数和它们的阶是相同的．一般地说，这对于有限的阿贝尔 p 群是对的，但是因为 6 阶循环群是 2 阶和 3 阶循环群的直积，对于不是 p 群的有限阿贝尔群这是不对的．如果 A 是阿贝尔 p 群，它是阶为 $p^{e_1},\cdots,p^{e_r}$ 的循环群的直积，则这些阶数叫做已知群的不变量．在全体不变量是 $p,\cdots,p$ 的特殊（但是重要的）情形，我们说 A 是初等阿贝尔群．明白地，一个阿贝尔群 A 的不变量在同构的意义下决定 A，然而它们还是在下列定理中明白指出的更强意义的不变量．

定理 3.3.2. 如果有限阿贝尔 p 群 A 以两种方式表示成循环群的直积 $A=A_1\times\cdots\times A_r=B_1\times\cdots\times B_s$，则它们的因子数相同 $r=s$，而且 $A_1,\cdots,A_r$ 的阶经过重新排列后与 $B_1,\cdots,B_s$ 的阶完全相同.

证明．我们对 A 的阶施行归纳法，当 A 的阶是素数 p 时定理是显然的．

设 A 是任意的阿贝尔 p 群．我们用 A_p 表示 A 中满足 $x^p=1$ 的元素 x 的子群，而且用 A^p 表示形状 $y^p(y\in A)$ 的元素的子群．设 A 的一个基底是 $a_1,\cdots,a_r$，这里 a_i 的阶是 p^{e_i}，$i=1,\cdots,r$，而且设 a 的编号是使得 $e_1\geqslant e_2\geqslant\cdots\geqslant e_r$．于是我们容易验证 A_p 有一个基底 $a_1^{p^{e_1-1}},\cdots,a_r^{p^{e_r-1}}$ 而且是 p^r 阶的．如果 A 是初等阿贝尔群，则 $A^p=1$．否则设 e_m 是最后一个大于 1 的方次数，即 $e_1\geqslant\cdots\geqslant e_m>e_{m+1}=\cdots=e_r=1$．那么 A^p 有一个基底 $a_1^p,\cdots,a_m^p$，这是容易证明的．

设 A 有另一个基底 $b_1,\cdots,b_s$，这里 b_i 的阶是 p^{f_i}，$i=1,\cdots,s$，而且 $f_1\geqslant f_2\geqslant\cdots\geqslant f_s$．那么 A_p 从基底 $a_1,\cdots,a_r$ 看是 p^r 阶的，而从基底 $b_1,\cdots,b_s$ 看则是 p^s 阶的，因而 $r=s$．如果 A 是初等阿贝尔群，这就完成了证明．否则设 $f_1\geqslant f_2\geqslant\cdots\geqslant f_n>f_{n+1}=\cdots=f_s=1$．那么 A^p 既有不变量 $p^{e_1-1},\cdots,p^{e_m-1}$，又有不变量 $p^{f_1-1},\cdots,p^{f_n-1}$．根据归纳假

设，$m=n$ 而且 $e_1-1=f_1-1, \cdots, e_m-1=f_m-1$. 由此并且根据 $s=r$ 的事实，就得出 $e_1=f_1, \cdots, e_r=f_r$，定理证明了.

推论 3.3.2. 如果两个有限阿贝尔 p 群不具有相同的不变量，则它们不是同构的.

定理 3.3.3. 具有不变量 $p^{e_1}, \cdots, p^{e_r}$, $e_1 \geqslant \cdots \geqslant e_r$ 的阿贝尔群 A 有子群 K 具有不变量 $p^{k_1}, \cdots, p^{k_t}, k_1 \geqslant \cdots \geqslant k_t$，必要而且只要 $t \leqslant r$ 和 $k_1 \leqslant e_1, \cdots, k_t \leqslant e_t$.

证明. 我们先对 A 的阶施行归纳法，来证明 A 的子群 K 的不变量的方次数满足定理里的不等式，当 A 的阶是 p 时这个定理显然成立.

因为 K_p 是 A_p 的子群，所以 $t \leqslant r$，当 A 是初等阿贝尔群时定理已经证明. 否则，设 $e_1 \geqslant \cdots \geqslant e_m > e_{m+1} = \cdots = e_r = 1$ 和 $k_1 \geqslant \cdots \geqslant k_u > k_{u+1} = \cdots = k_t = 1$. 那么 K^p 是 A^p 的子群而且 K^p 的不变量是 $p^{k_1-1}, \cdots, p^{k_u-1}$，$A^p$ 的不变量是 $p^{e_1-1}, \cdots, p^{e_m-1}$. 根据归纳假设，$u \leqslant m$ 和 $k_i-1 \leqslant e_i-1$, $i=1, \cdots, u$. 因此 $k_i \leqslant e_i$, $i=1, \cdots, u$，又因为 $k_{u+1}=\cdots=k_t=1$，所以还有 $k_i \leqslant e_i$, $i=u+1, \cdots, t$. 总之，$k_i \leqslant e_i$, $i=1, \cdots, t$.

如果定理中的不等式成立，则 A 有一个子群具有已知的不变量，这时我们可以取 A 的前 t 个基元素的适当方幂作为它的一个基底. 但是在一般情况下，以下的事实并不一定成立：给定 A 和子群 K，我们可以取 A 的基底和 K 的基底，使得 K 的基底由 A 的基元素的方幂组成.（参看习题5.）

习　　题

1. 设阿贝尔群 A 由具有定义关系 $a^3b^9c^9=1$ 和 $a^9b^{-3}c^9=1$ 的元素 a, b, c 生成. 求 A 的一个基底和基元素的阶.

2. 证明有限阿贝尔 p 群由它的最高阶的诸元素生成.

3. 设一个阿贝尔群具有不变量 p^3, p^2. 问它包含多少个 p^2 阶的子群?

4. 给出两个恰好包含 p^2+p+1 个 p 阶子群的阿贝尔 p 群.

5. 设 A 是由 a 和 b 生成的、具有定义关系 $a^{p^3}=1$ 和 $b^p=1$ 的阿贝尔群. 设 K 是由元素 $x=a^pb$ 生成的子群. 证明: 不可能选取 A 的基底和 K 的基底,使得 K 的基元素是 A 的基元素的方幂.

第四章　西 罗 定 理

4.1. 拉格朗日定理的逆定理不成立

根据拉格朗日定理，有限群的子群的阶是整个群的阶的约数．但是，在m是n的约数时，一个n阶群并不一定有m阶的子群．举例说，下面的12阶置换群就没有6阶子群：

$$\begin{pmatrix}1,2,3,4\\1,2,3,4\end{pmatrix}\qquad\begin{pmatrix}1,2,3,4\\1,3,4,2\end{pmatrix}$$

$$\begin{pmatrix}1,2,3,4\\2,1,4,3\end{pmatrix}\qquad\begin{pmatrix}1,2,3,4\\1,4,2,3\end{pmatrix}$$

$$\begin{pmatrix}1,2,3,4\\3,4,1,2\end{pmatrix}\qquad\begin{pmatrix}1,2,3,4\\3,2,4,1\end{pmatrix}$$

$$\begin{pmatrix}1,2,3,4\\4,3,2,1\end{pmatrix}\qquad\begin{pmatrix}1,2,3,4\\4,2,1,3\end{pmatrix}$$

$$\begin{pmatrix}1,2,3,4\\2,3,1,4\end{pmatrix}\qquad\begin{pmatrix}1,2,3,4\\2,4,3,1\end{pmatrix}$$

$$\begin{pmatrix}1,2,3,4\\3,1,2,4\end{pmatrix}\qquad\begin{pmatrix}1,2,3,4\\4,1,3,2\end{pmatrix}$$

然而它却有2，3和4阶的子群．

因此，一般地说，当m整除n时，我们不能保证n阶群有m阶子群．但是当m是素数或素数的方幂时，这样的子群是存在的．这种子群的存在和个数是下面的西罗定理的内容．我们从作为西罗定理的起点的一个定理开始．

定理 4.1.1.　如果群G的阶能被素数p整除，则G包含着

p 阶的元素.

证明. 设 $n = mp$ 是 G 的阶. 这时如果 $m = 1$, 则 G 是 p 阶循环群,因而定理成立. 我们对 m 施行归纳法.如果 G 包含一个真子群 H, 它的指数 $[G:H]$ 不能被 p 整除,则 H 的阶能被 p 整除,因而根据归纳假设,H 包含 p 阶的元素. 现在假定 G 的每个真子群的指数都能被 p 整除. 那么根据 §1.6, $n = n_1 + n_2 + \cdots + n_s$, 这里每个 n_i 都是 G 的共轭元素类的元素数. 每个 $n_i \neq 1$ 是 G 的一个真子群的指数, 因而根据假设都能被 p 整除. 这时 $n_1=1$, 因为单位元素自成一类. 因此 $n_i = 1$ 的个数是 p 的倍数. 在 G 内一个元素 a_i 自成一类,必要而且只要它属于 G 的中心 Z. 因此中心 Z 的阶能被 p 整除. 于是对于 $z \in Z$ 和 $g \in G$, 我们有 $zg = gz$. 因此当然更有 Z 的元素彼此都可交换, 即 Z 是阿贝尔群. 现在从定理 3.3.1 的推论得出, Z 包含 p 阶的元素.

4.2. 三个西罗定理

定理 4.1.1 保证,当 p 整除 G 的阶时, 至少存在一个 p 阶子群. 我们可以证明, 如果 G 的阶是 $n = p^m s$, 则还存在 p^2, p^3, $\cdots$, p^m 阶的子群.

定理 4.2.1 (第一个西罗定理). 如果 G 的阶是 $n = p^m s$, 这里 p 是素数, $p \nmid s$, 则 G 包含着阶为 $p^i (i = 1, \cdots, m)$ 的子群,而且阶为 $p^i (i = 1, \cdots, m-1)$ 的每个子群至少是一个 p^{i+1} 阶子群的正规子群.

证明. 对 i 施行归纳法来证. 上面已经说过, G 包含 p 阶子群. 设 P 是 $p^i (i \geqslant 1)$ 阶子群. 用 P 的二重傍系表出 G, $G = P + Px_2P + \cdots + Px_rP$, 而且设在 Px_jP 内有 P 的 a_j 个右傍系. 那么 $[G:P] = a_1 + a_2 + \cdots + a_r$, 这里 $a_j =$

$[x_j^{-1}Px_j : x_j^{-1}Px_j \cap P]$，而且对于二重傍系 $P \cdot 1 \cdot P = P, a_1 = 1$. 又 $a_j = 1$ 或 p 的方幂. 因为 $p \mid [G:P]$，所以等于 1 的 a_j 数必须是 p 的倍数. 如果 $a_j = 1$，则 $x_j^{-1}Px_j = P$，因而 x_j 以及傍系 $Px_j = x_jP$ 必须属于 P 的正规化子 K. 反之，如果 $x_j \in K$，则 $x_j^{-1}Px_j = P$，因而 $a_j = 1$. 因此 $[K: P]$ 是等于 1 的 a_j 数，所以 $p \mid [K: P]$. 因此商群 K/P 的阶 $[K: P]$ 能被 p 整除. 于是 K/P 包含一个 p 阶的子群 J^*. 根据定理 2.3.4，$J^* = J/P$，这里 $J \subseteq K$，而且 $[J: P] = [J^*: 1] = p$，因而 J 是包含 P 作为正规子群的 p^{i+1} 阶子群.

定义. 如果群 P 的除单位元素外的所有元素的阶都是素数 p 的方幂，则 P 叫做 p 群.

定义. 群 G 的子群 S 叫做 G 的西罗子群，假如它是 p 群而且不包含在作为 G 的子群的更大 p 群内.

我们使用以上定义的术语来写出第一个西罗定理的两个推论.

推论 4.2.1. 阶为 $n = p^m s$（p 是素数，$p \nmid s$）的每个有限群 G 包含着阶为 p^m 的西罗子群，而且作为 G 的子群的每一个 p 群总包含在 G 的西罗子群内.

阶为 p^m 的每个群是 p 群. 根据定理 4.1.1，如果一个群的阶能被两个不同的素数整除，则它不会是 p 群. 因此每一个有限 p 群的阶是 p 的方幂 p^m.

推论 4.2.2. p^m 阶 p 群 P 的每个真子群包含在阶为 p^{m-1} 的一个极大子群内，而且 P 的所有极大子群都是正规子群.

定理 4.2.2（第二个西罗定理）. 在有限群 G 内，西罗 p 子群都是共轭的.

证明. 设 P_1 和 P_2 是两个西罗 p 子群. 那么 $G = P_1P_2 + P_1x_2P_2 + \cdots + P_1x_sP_2$. 设在 $P_1x_iP_2$ 内有 P_2 的 b_i 个右傍系. 于是 $b_i = [x_i^{-1}P_1x_i: x_i^{-1}P_1x_i \cap P_2]$ 而且它是 1 或 p 的方幂. 但是

$b_1 + \cdots + b_s = [G: P_2]$ 不是 p 的倍数. 因此对于某个 i 有 $b_i = 1$, 于是 $x_i^{-1}P_1x_i = P_2$.

定理 4.2.3 (第三个西罗定理). 有限群 G 的西罗 p 子群的个数有形状 $1 + kp$, 而且是 G 的阶的约数.

证明. 如果只有一个西罗 p 子群, 定理是显然的. 设 S_0 是西罗 p 子群, 而 $S_1, \cdots, S_r$ 是其余的西罗 p 子群. 用 S_0 的元素作变形时, 这些子群分属于若干个不同的共轭类. 根据第二个西罗定理, S_i 是在它的正规化子 K_i 内的唯一的西罗 p 子群. 因此 S_i 在 S_0 内的正规化子 $(i \neq 0)$ 是 S_0 的一个真子群, 因而 S_i 在 S_0 下的共轭者的个数是 p 的方幂 $p^e, e \geqslant 1$. 因此 $r = p^{e_1} + \cdots + p^{e_r} = kp$, 即 G 有 $1 + r = 1 + kp$ 个西罗 p 子群. 根据第二个西罗定理, 西罗 p 子群的个数是 S_0 的正规化子的指数, 因而是 G 的阶的约数.

定理 4.2.4. 设 K 是西罗 p 子群 P 在有限群 G 内的正规化子. 那么具有性质 $G \supseteq H \supseteq K \supseteq P$ 的任何子群 H 是它自己在 G 内的正规化子.

证明. 假定 $x^{-1}Hx = H$. 那么 $H \supseteq x^{-1}Px = P'$, 它必定是 H 的西罗 p 子群. 因此, 对于某个 $u \in H$ 有 $u^{-1}P'u = P$, 于是 $u^{-1}x^{-1}Pxu = P$, 即 $xu \in K$. 因此 $x \in H$, 即 H 是它自己的正规化子.

下面一个定理不仅本身是有价值的, 而且在以后各章里有若干重要的应用.

定理 4.2.5 (伯恩赛德). 如果在有限群 G 内, p 群 h 在一个西罗 p 子群内是正规的, 而在包含它的其他西罗 p 子群内不是正规的, 则就存在 r 个 $[r > 1, r \not\equiv 0 \pmod{p}]$ 共轭的群 $h = h_1, \cdots, h_r$, 它们在 $H = h_1 \cup h_2 \cup \cdots \cup h_r$ 内都是正规的, 而在 G 的包含它们的任何西罗 p 子群内并不都是正规的. 于是 $h_1, \cdots, h_r$ 在 H 的正规化子 N_H 内组成一个完全的共轭

类.

证明. 设N_h是h的正规化子. 设Q是G的西罗p子群，使得h是Q的非正规的子群，而且$D=N_h\cap Q$是极大的.

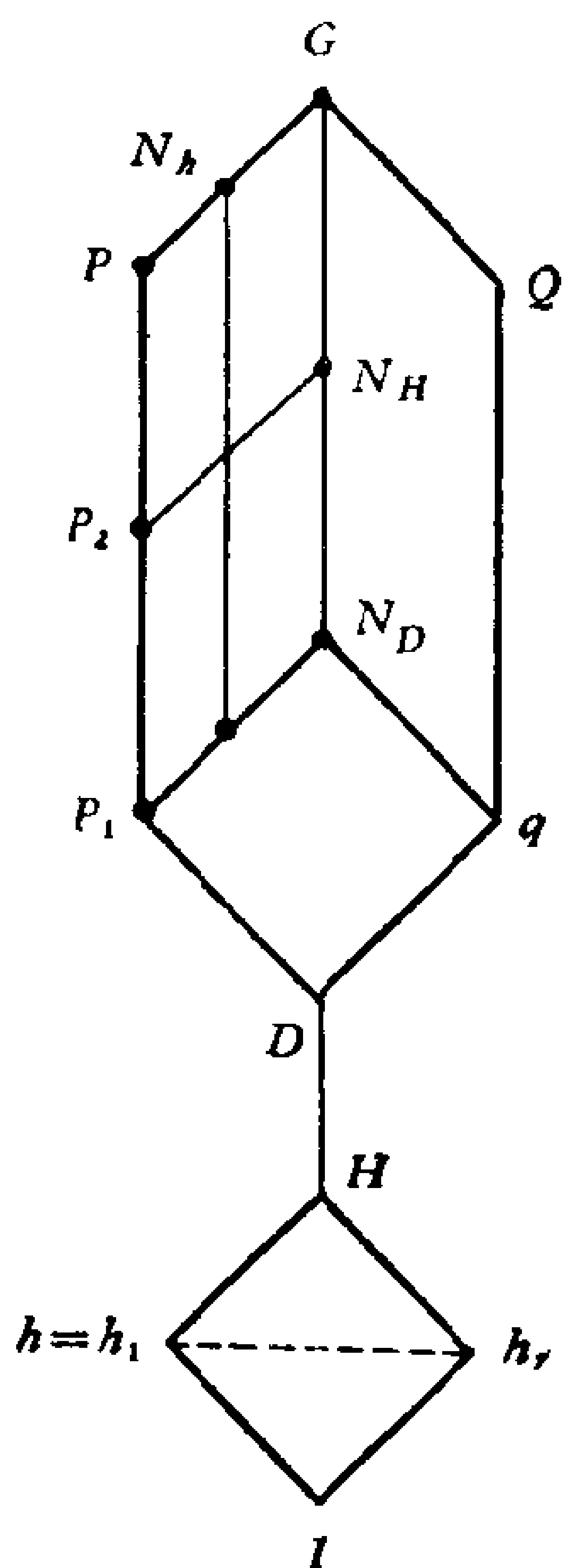


图 2 伯恩赛德定理

设q是D在Q内的正规化子，N_D是D在G内的正规化子. 我们可以断定$Q\supseteq q\supset D\supset h$，因为$h$在$Q$的某个子群内是正规的而且有指数$p$，而$h$在$Q$内是非正规的，所以$Q\supset D\supset h$. 再有，$Q$的真子群$D$是作为真子群而包含在它在$Q$内的正规化子$q$内的，因此$Q\supseteq q\supset D\supset h$. 现在因为$D=N_h\cap Q$，$h$在$q$内不是正规的，当然在$N_D$内也不是正规的. 设$h=h_1,\cdots,h_s(s>1)$是$h$在$N_D$内的共轭者. 因为$h$在$D$内是正规的，而且$N_D$导出$D$的自同构，所以每个$h_i$在$D$内也都是正规的，当然在$H=h_1\cup h_2\cup\cdots\cup h_s\subseteq D$内更是如此. H的正规化子N_H包含着N_D，因为N_D的元素把H变成自己.

设p_1是$N_h\cap N_D$的西罗子群，而$P_1\supseteq p_1$是N_h的西罗子群. 根据假设，P_1是G的西罗子群. 于是$D\subset p_1$因为D在P_1内不是自己的正规化子. 现在$N_h\cap N_D\subseteq N_D\subseteq N_H$，又设$p_2\supseteq p_1$是$N_H$的西罗子群，再设$P\supseteq p_2$是$G$的西罗子群. 如果$P\nsubseteq N_h$，则$P\cap N_h\supseteq p_1\supset D$，与$D$的极大性矛盾. 因此$P\subseteq N_h$，于是$N_h\cap N_H\supseteq P\cap N_H=p_2$，因为$p_2$是$N_H$的西罗子群.

设$h=h_1,\cdots,h_s,\cdots,h_r$是$h$在$N_H$内的共轭者(因而都是$H$的正规子群). h在N_H内的正规化子是$N_H\cap N_h$，因

而 h 在 N_H 内的共轭者的个数是 $r=[N_H: N_H\cap N_h]$. 但是 $N_H\cap N_h\supseteq p_2$, 而后者是 N_H 的西罗子群. 因此 $r\not\equiv 0(\bmod p)$.

如果全体 $h_1, \cdots, h_r$ 都是某个西罗子群 S_p 的正规子群, 则 $S_p\subseteq N_H$, 因而 N_H 的每个西罗子群包含全体 h_i 作为正规子群. 但是 $q\subseteq N_D\subseteq N_H$ 是 p 群,它并不以 h_1 作为正规子群.

4.3. 有 限 p 群

根据西罗定理, 阶为 $n=p_1^{e_1}\cdots p_r^{e_r}$ 的群 G 对于每个 i 包含 $p_i^{e_i}$ 阶的子群, 而且同是这个阶的所有子群都彼此同构, 因为它们是共轭的. 因此有限群的构造问题可以分成两部分: 1) 构造阶为素数方幂的群; 2) 把阶为整除 n 的素数方幂的群联合起来而构成 n 阶的群. 当全体西罗子群都是循环群时 (全体 $e_i=1$ 当然是这样一种情形), 我们可以解决第二个问题, 解答在第 9 章里给出 (定理 9.4.3). 因此, 虽然这两个问题一般地说还没有得到解决, 但是我们必须解决第一个问题以便获得在第二个问题里用到的子群. 要把西罗子群联合起来构造成群的最大困难, 看来是在于构造阶为素数方幂的群 (即所谓 p 群) 时的复杂性.

关于 p 群的第一个有很大价值的事实是以下的

定理 4.3.1. 有限 p 群的中心总比单位元素群大.

证明. 设 P 是有限 p 群, 我们把 P 表成共轭类的和:

$$P=C_1+C_2+\cdots+C_r. \tag{4.3.1}$$

这里 C_1 单由单位元素组成. 设 h_i 是 C_i 的元素数, 根据定理 1.6.1, 它是 P 的子群的指数,因而当 C_i 包含中心的元素时是 1,否则是 p 的方幂. 但是因为 P 的阶是 p^m, 我们必须有

$$p^m=h_1+h_2+\cdots+h_r. \tag{4.3.2}$$

这里 $h_1=1$, 因而在 (4.3.2) 内其余的 h_i 不可能都是 p 的真

方幂，即必定还有其他 h_i 等于 1，所以 P 的中心比单位元素群大.

我们把推论 4.2.2 改写成一个定理.

定理 4.3.2. 阶为 p^m 的 p 群 P 的每个真子群总包含在阶为 p^{m-1} 的极大子群内，而且 P 的所有极大子群都是正规子群.

(第一个) 西罗定理 4.2.1 的又一个推论是：p 群的真子群不会是它自己的正规化子.我们现在来证明这个事实的逆.

定理 4.3.3. 有限群 G 的真子群都不是自己的正规化子，必要而且只要 G 是它的西罗子群的直积.

证明. 假定 G 的真子群都不是自己的正规化子. 根据定理 4.2.4，西罗子群 P 的正规化子 K 是它自己的正规化子，因而根据假设，K 必须是整个群 G. 因此 P 是 G 的正规子群. 由此根据定理 2.5.2，西罗子群的并是西罗子群的直积，所以 G 是它的西罗子群的直积. 现在假定 $G = P_1 \times \cdots \times P_r$，这里 P_i 是阶为 $p_i^{e_i}$ 的群而且 $p_i \neq p_j$ 对于 $i \neq j$.现在如果 $g = g_1g_2\cdots g_r$，$g_i \in P_i$，则引理 3.2.2 的条件成立，因而每个 g_i 是 g 的一个方幂. 因此，对于 G 的子群 H 的元素 g，它的每个分量 g_i 也是 H 的元素.因而 H 本身必须是一个直积 $H = H_1 \times \cdots \times H_r$，这里 $H_i = H \cap P_i$ 是 P_i 的子群. 如果 H 是 G 的真子群，则有某个 H_j 是 P_j 的真子群，于是把这个 H_j 换成它在其中是正规子群的 P_j 的更大子群，我们就将得出一个比 H 大的子群，H 在其中是正规的.

定理 4.3.4. 如果 A 是包含在 p 群 P 内的 p 阶正规子群，则 A 包含在 P 的中心内.

证明. p 阶群 A 是由一个元素 a 生成的循环群，它的元素是 $1, a, \cdots, a^{p-1}$. 因为 A 是正规的，元素 a 的共轭者包含在集合 $a, a^2, \cdots a^{p-1}$ 内. 但是 a 的共轭者数是它的中心化

子的指数，因而是 1 或 p 的方幂．而现在共轭者的个数最多是 $p-1$，它只能是1，因而 a 以至整个 A 都在 P 的中心内．

4.4. 阶为 p, p^2, pq, p^3 的群

阶为素数 p 的群不能有真子群，因而必定是由不是单位元素的任何元素生成的循环群．我们在定理 1.5.4 里已经证明过，没有任何真子群的群 G 是素数阶的循环群．

阶为 p^2 的群 G，如果不是循环群，就要包含两个 p 阶子群 $\{a\}$ 和 $\{b\}$，这里 $a^p=1$，$b^p=1$，而且 $\{a\}\cap\{b\}=1$．因为这两个都是极大子群，根据推论 4.2.2，它们都是正规的，因而根据定理 3.2.1，$G=\{a\}\times\{b\}$；所以 G 是以 a，b 为基底的阿贝尔群．

假定 G 的阶是 pq，这里 $p<q$ 是素数．根据第三个西罗定理，q 阶子群的个数有形状 $1+kq$ 而且能整除 p，因而它必须是 1，而且这唯一的 q 阶子群是正规的，设它是 $\{b\}$，这里 $b^q=1$．p 阶子群的个数有形状 $1+kp$ 而且能整除 q，因而它是 1 或 q． 如果这个数是 1，则我们有一个正规子群 $\{a\}$，这里 $a^p=1$，而且 G 是 $\{a\}$ 和 $\{b\}$ 的直积．这时 $c=ab$ 的阶是 pq，因而 G 是循环群．剩下的是有 $1+kp=q$ 个 p 阶子群的情形，这时有一个 p 阶子群 $\{a\}$ 不是正规的．于是我们有

$$a^p=1, \quad b^q=1,$$

而且因为 $\{b\}$ 是正规的，对于某个 r 有 $a^{-1}ba=b^r$．这时如果 $r=1$，则 G 是阿贝尔群，即是上面说过的循环群．因此 $r\neq 1$．于是对于任何 i 有 $a^{-1}b^ia=b^{ir}$，而且特别地有 $a^{-1}b^ra=b^{r^2}$，因而 $a^{-2}ba^2=a^{-1}b^ra=b^{r^2}$． 更一般可以用归纳法证明 $a^{-j}ba^j=b^{r^j}$．因此对于 $j=p$，我们有 $b=a^{-p}ba^p=b^{r^p}$，因

而 $r^p \equiv 1 \pmod{q}$. 关于 r 的这个必要条件也是充分的. 为了证明这一点，只要确立两个元素相乘时的下列一般规则

$$(a^u b^v)(a^x b^y) = a^{u+x} b^{vr^x+y},$$

并且证明这个规则决定一个 pq 阶群. 这是将在定理 6.5.1 里确立的更一般的规则的特别情形.

对于阶为 p^3 的群有三种类型的阿贝尔群，它们的不变量分别是 (p^3), (p^2, p) 和 (p, p, p). 为了寻求非阿贝尔群，我们把 $p = 2$ 和奇数 p 的情形分开. 先设 $p = 2$ 来考虑 8 阶的非阿贝尔群. 这时不能有 8 阶的元素，因为否则将得出循环群. 如果所有非单位元素都是 2 阶的，则 $(ab)^2 = 1$ 或 $abab = 1$, $ba = a^2bab^2 = ab$, 得到阿贝尔群. 因此必须有 4 阶元素 a, $a^4 = 1$. 如果 $b \notin \{a\} = A$[1], 则 $G = A + Ab$ 而且 $b^2 \in A$. 如果 $b^2 = a$ 或 a^3, 则 b 是 8 阶的因而 G 是循环群. 因而 $b^2 = 1$ 或 a^2. 又因为 A 是正规的, $b^{-1}ab \in A$, 于是 $b^{-1}ab = a$ 或 a^3, 因为它是 4 阶元素. 但是当 $b^{-1}ab = a$ 时 G 是阿贝尔群. 因此 $b^{-1}ab = a^3$. 于是我们找出两个非阿贝尔群：具有定义关系

$$a^4 = 1, \quad b^2 = 1, \quad b^{-1}ab = a^3$$

的二面体群和具有定义关系

$$a^4 = 1, \quad b^2 = a^2, \quad b^{-1}ab = a^3$$

的四元素群. 容易验证这些关系定义两个 8 阶群，而且它们彼此不同构.

最后来考虑 p 为奇素数时的 p^3 阶非阿贝尔群. 因为 G 不是循环群，它不包含 p^3 阶的元素. 先假定 G 包含 p^2 阶的元素 a, $a^{p^2}=1$. 那么 $\{a\}=A$ 作为极大子群是正规的. 设 $b \notin A$. 那么 $G = A + Ab + \cdots + Ab^{p-1}$, 而且 $b^p \in A$, $b^{-1}ab=a^r$.

1) 原书误排为 $b \in \{a\} = A$.——译者

这时 $r \neq 1$，因为G是非阿贝尔群．对 j 施行归纳法可以得出 $b^{-j}ab^j = a^{r^j}$，又因为 b^p 作为A的元素与 a 可交换，我们有 $a = b^{-p}ab^p = a^{r^p}$，因而 $r^p \equiv 1\ (\mathrm{mod} p^2)$．根据费尔马定理，$r^p \equiv r(\mathrm{mod} p)$，所以 $r \equiv 1(\mathrm{mod} p)$．记 $r = 1 + sp$．那么只要选取 j 使得 $js \equiv 1(\mathrm{mod} p)$，我们就有

$$b^{-j}ab^j = a^{(1+sp)j} = a^{1+sjp} = a^{1+p}.$$

因为 $(j,p) = 1$，$b^j \notin A$，我们可以用 b^j 代替 b 来得出

$$G = A + Ab + \cdots + Ab^{p-1},$$

这里 $b^{-1}ab = a^{1+p}$.

现在因为 $b^p \in A$，所以 $b^p = a^t$．这时因为 b 的阶不是 p^3，t 必须是 p 的倍数．记 $b^p = a^{up}$．于是利用关系 $a^ib = ba^{i(1+p)}$，我们经过计算得出

$$\begin{aligned}(ba^{-u})^p &= b^pa^{-u[1+(1+p)+(1+p)^2+\cdots+(1+p)^{p-1}]}\\ &= b^pa^{-up-up(1+2+\cdots+p-1)}\\ &= b^pa^{-up} = 1.\end{aligned}$$

这里我们用到了下列事实：因为 p 是奇数，$1 + 2 + \cdots + p - 1 = p(p-1)/2$ 是 p 的倍数．现在我们取 $b_1 = ba^{-u}$，就有关系 $a^{p^2} = 1$，$b_1^p = 1$，$b_1^{-1}ab_1 = a^{1+p}$．最后这个关系是因为 $b_1^{-1}ab_1 = a^u(b^{-1}ab)a^{-u}$.

作为最后一种情形，假定G不包含 p^2 阶的元素．这时中心Z必定是 p 阶的，因为如果它的阶至少是 p^2，则G就将是阿贝尔群．G/Z 的类型是 $x^p = 1$，$y^p = 1$，$yx = xy$．如果在同态 $G \to G/Z$ 下，$a \to x$，$b \to y$，则 $a^p = 1$，$b^p = 1$，$a^{-1}b^{-1}ab = c \in Z$．如果 $a^{-1}b^{-1}ab = 1$，则因为 a，b 和 Z 生成 G，G 就将是阿贝尔群．因此 $c \neq 1$ 是Z的生成元素，而且定义关系成为

$$a^p = 1,\ b^p = 1,\ c^p = 1,\ ab = bac,\ ac = ca,\ bc = cb.$$

定义关系表.

I. G 的阶是p.

1）循环群. $a^p = 1$.

II. G 的阶是 p^2.

1）循环群. $a^{p^2} = 1$.

2）初等阿贝尔群. $a^p = 1, b^p = 1, ba = ab$.

III. G 的阶是 pq，$p < q$.

1）循环群. $a^{pq} = 1$.

2）非阿贝尔群. $a^p = 1$，$b^q = 1$，$a^{-1}ba = b^r$，

$r^p \equiv 1(\mathrm{mod}q)$，$r \not\equiv 1(\mathrm{mod}q)$，$p$ 整除 $q - 1$.

方程 $z^p \equiv 1(\mathrm{mod}q), z \not\equiv 1(\mathrm{mod}q)$ 的解是 r，r^2，$\cdots$，r^{p-1}，而且产生同一个群，因为用 a^j 代替 a 作为 $\{a\}$ 的生成元素，r 就换成 r^j.

IV. G 的阶是 p^3，

阿贝尔群.

1）$a^{p^3} = 1$.

2）$a^{p^2} = 1$，$b^p = 1$，$ba = ab$.

3）$a^p = b^p = c^p = 1$，$ba = ab$，$ca = ac$，$cb = bc$.

非阿贝尔群，阶是 $2^3 = 8$.

4）二面体群. $a^4 = 1$，$b^2 = 1$，$ba = a^{-1}b$.

5）四元数群. $a^4 = 1$，$b^2 = a^2$，$ba = a^{-1}b$.

非阿贝尔群，阶是 p^3，p 是奇数.

4）$a^{p^2} = 1$，$b^p = 1$，$b^{-1}ab = a^{1+p}$.

5）$a^p = 1$，$b^p = 1$，$c^p = 1$，$ab = bac$，

$ca = ac$，$cb = bc$.

习　　题

1. 证明，如果H是有限群G的正规子群而且$[G:H]$是素数p，则H包含G的每个西罗p子群。
2. 证明，群G内阶为p^a的正规子群K包含在G的每个西罗p子群内。
3. 证明，当p和q是不同的素数时，p^2q阶的群必定包含正规的西罗子群。
4. 证明，阶为200的群必定包含正规的西罗子群。
5. 在不包含正规子群的168阶群内包含多少个7阶元素？
6. 在下面的表内列举了从1到20阶的不同的群的个数。验证除16外的各个阶的情形。

阶	1	2	3	4	5	6	7	8	9	10
群　　数	1	1	1	2	1	2	1	5	2	2
阶	11	12	13	14	15	16	17	18	19	20
群　　数	1	5	1	2	1	14	1	5	1	5

第五章 置 换 群

5.1. 圈[1)]

在第一章的凯雷定理里指出，每个群都可以表示成一个置换群. 那时还指出，同一个群可以用不同的方式表示成置换群. 对于一个置换 π, 我们用 $(x_i)\pi = x_j$ 表示 π 把 x_i 变成 x_j.

有限圈是指有限集合 $x_1, x_2, \cdots, x_n$ 的这种置换 π, 使得 $(x_1)\pi = x_2, \cdots, (x_{n-1})\pi = x_n, (x_n)\pi = x_1$.

无限圈是指无限集合 $x_i, i = -\infty, \cdots, +\infty$ 的这种置换 π, 使得 $(x_i)\pi = x_{i+1}, i = -\infty, \cdots, +\infty$.

我们用 $(x_1, x_2, \cdots, x_n)$ 表示有限圈，用 $(\cdots, x_{-1}, x_0, x_1, \cdots)$ 表示无限圈. 显然，圈 $(x_2, \cdots, x_n, x_1)$ 和圈 $(x_1, x_2, \cdots, x_n)$ 是同一个置换.

定理 5.1.1. 给了集合 S 的任意置换 π. 集合 S 可以分成互不相交的子集，使得 π 在每个子集上都是圈.

证明. 设 x_1 是集合 S 的任意元素. 如果 $(x_1)\pi = x_1$, 则 (x_1) 本身是一个圈. 如果 $(x_1)\pi \neq x_1$, 记 $(x_1)\pi = x_2$. 然后记 $(x_2)\pi = x_3, \cdots, (x_i)\pi = x_{i+1}$, 无限地继续下去，除非有一个元素重复出现. 如果 $(x_1)\pi = x_2, \cdots, (x_{n-1})\pi = x_n$ 都是不同的，但是 $(x_n)\pi$ 是上述元素中的一个，则对于某个 $i = 1, \cdots, n$ 有 $(x_n)\pi = x_i$. 如果 $i = 2, \cdots, n$ 中的一个，则

1) 圈也叫做循环置换.——译者

还有 $(x_{i-1})\pi = x_i$, 与 $x_n \neq x_{i-1}$ 的假设矛盾.因此 $(x_n)\pi = x_1$, 而我们就得出作为 π 对 $x_1, \cdots, x_n$ 作用的有限圈 $(x_1, \cdots, x_n)$. 如果 $(x_1)\pi^i = x_{i+1}$ $(i = 1, \cdots)$ 都是不同的，那么设 x_0 是使得 $(x_0)\pi = x_1$ 的元素. 用 $(x_{i-1})\pi = x_i$, $i = 0, -1, -2, \cdots$ 逐个定义 $x_{-1}, x_{-2}, \cdots$. 这些都是不同的,因为 π 不能把两个不同的元素变成同一个元素.因此，S 的每个 x 是在 π 下组成圈的某组元素中的一个. 然而因为在 $(x)\pi = y$ 中 x 和 y 的任何一个都唯一决定另一个，显然，整个圈由其中的任何一个元素决定. 因此不同的圈是不相交的.

于是我们可以把一个置换 π 表示成一连串的圈，而且由于这些圈作用于互不相交的元素集合，写出这些圈时的次序显然是没有关系的. 习惯上略去了长度为 1 的圈，因而所有略去的元素是固定的. 于是 $\pi = (1)(2)(3, 4, 5) = (3, 4, 5)$. 在这种规定下，一个置换在它所包含的圈数是有限的时候，可以看作是它的圈的乘积.

定理 5.1.2. 置换 π 的阶是它的圈的长度的最小公倍数.

证明. 在圈 $(x_1, \cdots, x_n)$ 内，$(x_i)\pi^j = x_{i+j}$, 这里 $i + j$ 已经取模 n 而简化. 因此 $(x_i)\pi^t = x_i$, 必要而且只要 t 是 n 的倍数. 因此 $(x_i)\pi^m = x_i$ 对于所有 $x_i \in S$, 必要而且只要 m 是 π 的每个圈的长度的倍数. 这时 $\pi^m = 1$. 如果 π 包含无限长的圈或任意长的圈，则 π 是无限阶的.

以下在计算时是很有用的公式:

引理 5.1.1. 如果

$$T = (a_{11}, \cdots, a_{1r})(a_{21}, \cdots, a_{2s})\cdots(a_{m1}, \cdots, a_{mt}),$$

而且 $$S = \begin{pmatrix} a_{11}, \cdots, a_{1r}, a_{21}, \cdots, a_{2s}, \cdots, a_{m1}, \cdots, a_{mt} \\ b_{11}, \cdots, b_{1r}, b_{21}, \cdots, b_{2s}, \cdots, b_{m1}, \cdots, b_{mt} \end{pmatrix},$$

则 $$S^{-1}TS = (b_{11}, \cdots, b_{1r})(b_{21}, \cdots, b_{2s})\cdots(b_{m1}, \cdots, b_{mt}).$$

证明. 取典型元素 b_{jk}, 我们有

$$b_{jk} \xrightarrow{S^{-1}} a_{jk} \xrightarrow{T} a_{j,k+1} \xrightarrow{S} b_{j,k+1},$$

所以在 $S^{-1}TS$ 下，$b_{jk} \to b_{j,k+1}$.

一个集合的全体置换的群叫做对称群. n 个文字上的对称群常常记做 S_n.

定理 5.1.3. 在对称群内两个元素共轭，必要而且只要它们的同一长度的圈数相同.

证明. 条件的必要性从上述引理的证明得出. 为了证明充分性，假定

$$T = (a_{11}, \cdots, a_{1r})(a_{21}, \cdots, a_{2s})\cdots(a_{m1}, \cdots, a_{mt}),$$

和 $$R = (b_{11}, \cdots, b_{1r})(b_{21}, \cdots, b_{2s})\cdots(b_{m1}, \cdots, b_{mt}),$$

这时把长度为 1 的圈也包括在内. 因为根据假设，T 和 R 的同一长度的圈数相同，所以我们可以假定它们的圈以相同的指标表出. 于是

$$Q = \begin{pmatrix} a_{11}, & \cdots, & a_{1r}, & \cdots, & a_{m1}, & \cdots, & a_{mt} \\ b_{11}, & \cdots, & b_{1r}, & \cdots, & b_{m1}, & \cdots, & b_{mt} \end{pmatrix}$$

就是使 $Q^{-1}TQ = R$ 的置换. 注意这个定理并未附加任何有限性条件，而且“个数相同”的意义也可以是指基数. 我们必须把长度为 1 的圈包括在内，这是因为如果考虑的元素数是无限的，则尽管 T 和 R 的长度大于 1 的圈的个数相同，但是它们可以固定不同个数的元素. 例如 $T=(0,1)(2,3)(4,5)\cdots$ 和 $R=(0)(1,2)(3,4)(5,6)\cdots$ 在数字 0, 1, 2, 3, …上的对称群内就不是共轭的.

5.2. 传 递 性

定理 5.2.1. 设 G 是文字 $x_1, \cdots, x_n$ 上的一个置换群. 设 S 是这些文字的任意子集. 那么 G 中不变 S 的全体文字的置换组成一个子群 K. 又把 S 的文字互相变换的置换也组成

一个子群 H，它包含K作为一个正规子群。

证明．如果两个置换 a 和 b 把 S 的文字互相变换，或不变 S 的文字，则乘积 ab 和逆 a^{-1} 也是如此．因此存在把 S 的文字互相变换的子群H和不变 S 的文字的子群 K．如果 $h\in H$，$k\in K$，则 $h^{-1}kh$ 不变 S 的文字，因而K是H 的正规子群．

定义．文字 $x_1,\cdots,x_n$ 上的置换群G说是在 $x_1,\cdots,x_n$的子集 S 上传递的，假如对于每个 $\sigma\in G$和 $x_i\in S$ 都有$(x_i)\sigma\in S$，而且对于 $x_i,x_j\in S$，存在$\sigma\in G$，使得 $(x_i)\sigma=x_j$．集合 S 叫做传递组．

定理 5.2.2. 如果对于固定的文字 x_1，集合 S 由全体 $x_i=(x_1)\sigma$，$\sigma\in G$ 组成，则 S 是一个传递组．

证明．如果 $(x_1)\sigma=x_i$，$(x_1)\tau=x_j$，则 $(x_i)\sigma^{-1}\tau=x_j$．其次，如果 $(x_1)\sigma=x_i$，$(x_i)\rho=x_k$，则 $(x_1)\sigma\rho=x_k$．

定理 5.2.3. 如果 S 是置换群G的传递组，而且 x_1 是 S 的文字，对于每个 $x_i\in S$ 取 $\sigma_i\in G$ 满足 $(x_1)\sigma_i=x_i$．设H是不变 x_1 的G的子群．那么 $G=H\sigma_1+\cdots+H\sigma_i+\cdots$

证明．如果 $g=h\sigma_i$，$h\in H$，则 $(x_1)g=x_i$，因而傍系 $H\sigma_i$ 互不相同．其次，设 g 是G的任意文字．那么对于某个 $x_i\in S$ 有 $(x_1)g=x_i$．于是 $(x_1)g\sigma_i^{-1}=x_1$，因而 $g\sigma_i^{-1}\in H$，$g=h\sigma_i\in H\sigma_i$，所以傍系 $H\sigma_i$ 穷尽了 G．

推论 5.2.1. 如果 S 是G的包含 r 个文字的传递组，则不变 S 的一个固定文字的子群H在G内的指数是 r．

定义．群G说是在集合 S 上 k 重传递的，假如它是在 S 上传递的，而且 S 的任何 k 个不同文字的有序集合被G的某个元素变成 S 的任意取定的 k 个不同文字的有序集合．

对 k 重传递群成立的有定理 5.2.2 的同类物．如果 G 把固定的 k 个文字 x_1，x_2，$\cdots$，x_k 变成 S 的文字的任意有序集

合 $y_1, y_2, \cdots, y_k$，则G是在S上k重传递的. 又G的不变S的$r<k$个文字的子群是在S的其余的文字上$k-r$重传递的. 又如果G是r重传递的，而且有一个不变r个文字的子群H本身是s重传递的，则G是$r+s$重传递的.

5.3. 用置换表示群

曾经说过一个抽象群可以用几种方式表示成置换群. 我们将把置换群P叫做G的一个表示，如果存在从G到P上的映射$g \to \pi(g)$，$g \in G$，$\pi(g) \in P$，使得$\pi(g_1)\pi(g_2)=\pi(g_1g_2)$. 因而$P$必定是$G$的同态像. 如果$P$确实同构于$G$，则我们说$P$是$G$的一个一一的表示. 正如$G$的所有同态像都由$G$对一个正规子群的商群给出，$G$的所有传递的置换表示可以用子群的左傍系表出.

因为6阶的非阿贝尔群可以一一地表示成三个文字上的一个传递的置换群或六个文字上的一个传递的置换群，我们必须区别作为抽象群看是同构的置换群.

定义. 集合S_1上的置换群P_1说是作为置换群而同构于集合S_2上的置换群P_2，假如存在P_1和P_2之间的同构$\pi_{p_1} \longleftrightarrow \pi_{p_2}$以及$S_1$和$S_2$之间的一一对应$x_i \longleftrightarrow y_i$，使得$(x_i)\pi_{p_1}=x_j$必要而且只要$(y_i)\pi_{p_2}=y_j$.

定理 5.3.1. 给了群G和子群H.

a）对于每个$g \in G$，存在H的左傍系的置换:

$$\pi(g)=\begin{pmatrix} Hx \\ Hxg \end{pmatrix}, x \in G.$$

b）$g \to \pi(g)$是把G表成H的不同左傍系的集合上的传递置换群的表示，而且$\pi(g)$不变H，必要而且只要$g \in H$.

反之，假定$g \to \pi(g)$是把G表成文字集合S上的传递置

换群 P 的表示.

c) 如果 s_1 是 S 的一个固定文字，则使 $\pi(g)$ 不变 s_1 的 g 组成 G 的子群 H.

d) S 的文字可以与 H 的左傍系成一一对应，使得 P 作为置换群而同构于在 a) 和 b) 里给出的置换 $\pi(g)$ 的群.

证明. a) $Hx \to (Hx)g = Hxg$ 把每个左傍系 Hx 变成唯一的左傍系 Hxg. 因为 $(Hxg^{-1})g = Hx$, $\pi(g) = \begin{pmatrix} Hx \\ Hxg \end{pmatrix}$ 是 H 的不同左傍系的集合的置换.

b) 因为 $(Hxg_1)g_2 = Hx(g_1g_2)$, 所以 $\pi(g_1)\pi(g_2) = \pi(g_1g_2)$, 因而 $g \to \pi(g)$ 是 G 的一个表示. $H \to Hg = H$, 必要而且只要 $g \in H$. 换句话说，$\pi(g)$ 不变 H, 必要而且只要 $g \in H$. 因为在 $\pi(x)$ 下 $H \to Hx$, 所以这表示是传递的.

c) 我们直接验证使 $(s_1)\pi(g) = s_1$ 的 g 组成一个子群 H, 因为如果 g_1 和 g_2 具有这个性质，则 g_1g_2 和 g_1^{-1} 也是如此.

d) 使 $(s_1)\pi(g) = s_i$ 的 g 的集合不是空的，因为 P 是传递的. 如果把这种 g 中的一个记做 x_i, 则立即得出整个集合是左傍系 Hx_i, 这里 H 是在 c) 中提出的不变 s_1 的子群. 反之，左傍系 Hx 的全体元素具有相同的性质：它们所对应的置换都把 s_1 变成同一个像. 这就确立了在 S 的文字和 H 的左傍系之间的一一对应 $s_i \rightleftarrows Hx_i$. 设 P_1 是由 a) 和 b) 给定的 H 的左傍系的置换群，P_1 的置换是 $\pi_1(g) = \begin{pmatrix} Hx \\ Hxg \end{pmatrix}$, $g \in G$.

如果在 P 内有 $(s_i)\pi(g) = s_j$, 则 $(s_1)[\pi(x_i)\pi(g)] = s_j$, 于是 $x_ig \in Hx_j$, 因而 $(Hx_i)g = Hx_j$; 反之从这个关系得出 $(s_i)\pi(g) = s_j$. 因此，$s_i\pi(g) = s_j$, 必要而且只要 $Hx_i\pi_1(g) = Hx_j$. 特别地，$\pi(g)$ 是单位元素，必要而且只要 $\pi_1(g)$ 是单位元素. 因此 P 和 P_1 都是 G 的同态像，它们具有相同的核，而且 $\pi(g) \rightleftarrows \pi_1(g)$ 是在 P 和 P_1 之间的同构. 再由于 $s_i \rightleftarrows Hx_i$

是在 S 和 H 的左傍系的集合之间的一一对应，我们就确定 P 是作为置换群而同构于 P_1 的，这是因为 $(s_i)\pi(g) = s_j$ 必要而且只要 $Hx_i\pi_1(g) = Hx_j$.

根据这个定理，我们可以把群 G 的任何传递的置换表示说成是相对于一个子群 H 的表示. 如果 H 是单位元素群，则这表示就是在 §1.4 里给过的右正则表示.

定理 5.3.2. 在定理 5.3.1 的表示 $g \to \pi(g)$ 下，映成单位元素的元素组成 G 的包含在 H 内的最大正规子群，因而这表示是一一的，必要而且只要 H 不包含 G 的大于单位元素群的正规子群.

证明. 对于什么 g，$\pi(g)$ 才是单位元素？这时对于所有 $x \in G$，$Hxg = Hx$. 因此 $x^{-1}Hxg = x^{-1}Hx$ 或 $g \in x^{-1}Hx$. 于是 $g \in \bigcap_x x^{-1}Hx = N$. 这里 N 显然是包含在 H 内的 G 的正规子群. 其次，G 的包含在 H 内的任何正规子群包含在每个 $x^{-1}Hx$ 内，因而也包含在 N 内. 因此 N 是 G 的包含在 H 内的最大正规子群. 反之，如果 $g \in N$，则对于每个 x，$Hxg = Hx$. 因而 $\pi(g) = 1$. 所以 $N = 1$ 是 G 的表示 $g \to \pi(g)$ 的一一性的必要而且充分的条件.

推论 5.3.1. 阿贝尔群的唯一传递的一一表示是正则表示.

定理 5.3.3. G 相对于子群 H_1 和 H_2 的两个一一的表示是作为置换群而同构的，必要而且只要存在 G 的自同构 α，使得 $H_1^\alpha = H_2$.

证明. 如果 α 是 G 的自同构，使得 $H_1^\alpha = H_2$，则

$$H_1x \rightleftarrows H_1^\alpha x^\alpha = H_2x^\alpha$$

是在 H_1 和 H_2 的傍系之间的一一对应，使得当 $g \to \pi_1(g)$ 是相对于 H_1 的表示，而且 $g \to \pi_2(g)$ 是相对于 H_2 的表示时，就有

$$\pi_1(g) \rightleftarrows \pi_2(g^\alpha).$$

另一方面，假定存在一个置换同构

$$\pi_1(g) \rightleftarrows \pi_2(g^*).$$

因为表示是一一的，这决定一个一一对应，$g \rightleftarrows g^*$，它是G的一个自同构 β. 在置换同构 $\pi_1(g) \rightleftarrows \pi_2(g^*)$ 下，我们有$H_1 \rightleftarrows H_2u$. 因此，如果 $H_1g = H_1$，则

$$H_2ug^\beta = H_2u$$

或

$$u^{-1}H_2ug^\beta = u^{-1}H_2u,$$

反之亦然．因此如果 $g \in H_1$，则 $g^\beta \in u^{-1}H_2u$，反之亦然．于是$H_1^\beta = u^{-1}H_2u$，即 $H_2 = uH_1^\beta u^{-1} = H_1^\alpha$，这里 α 是G的一个自同构.

5.4. 交 替 群 A_n

考虑 n 个变数的多项式 $\Delta = \prod_{i<j}(x_i - x_j)$；$i$，$j \leqslant n$；$n \geqslant 2$. 如果 $x_1, x_2, \cdots, x_n$ 作了一次置换，则 Δ 变成 Δ 或 $-\Delta$. 把Δ写出是

$$\begin{aligned}\Delta = (x_1 - x_2)(x_1 - x_3)\cdots(x_1 - x_n)\cdot \\ (x_2 - x_3)\cdots(x_2 - x_n) \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ \cdot(x_{n-1} - x_n),\end{aligned}$$

我们看到对换 (x_1, x_2) 把 $x_1 - x_2$ 变成 $x_2 - x_1 = -(x_1 - x_2)$，把第一行的其余各个因子与第二行的因子对换，而剩下的因子不变．因此置换 (x_1, x_2) 把Δ变成 $-\Delta$. 我们把保留Δ不变的置换叫做偶置换，而把变Δ为 $-\Delta$的置换叫做奇置换.

定理 5.4.1. $x_1, x_2, \cdots, x_n$ 的偶置换在对称群 S_n 中组成

指数为 2 的正规子群．这个群叫做交替群 A_n.

证明．我们可以直接验证两个偶置换的乘积是偶置换，两个奇置换的乘积是偶置换，一个偶置换和一个奇置换的任何次序的乘积是奇置换．又恒同置换是偶置换．

因此 S_n 的偶置换组成一个子群 A_n．因为 (x_1, x_2) 是奇置换，傍系 $A_n(x_1, x_2)$ 整个由奇置换组成．但是如果 π 是一个置换，则 π 和 $\pi \cdot (x_1, x_2)$ 中一个是偶置换，另一个是奇置换．因为 $\pi = [\pi \cdot (x_1, x_2)] \cdot (x_1, x_2)$，所以 A_n 和 $A_n(x_1, x_2)$ 穷尽了 S_n 的元素，因而 $S_n = A_n + A_n(x_1, x_2) = A_n + (x_1, x_2)A_n$．因此 A_n 在 S_n 内的指数是 2，而且是一个正规子群．

长度为 2 的圈 (x_i, x_j) 叫做对换．S_n 内的所有对换都与(x_1, x_2) 共轭(定理 5.1.3)．但是不管 π 是什么，π 和π^{-1}的奇偶性相同，因而 $\pi^{-1}(x_1, x_2)\pi = (x_i, x_j)$ 是奇置换．我们也可以直接算出每个对换 (x_i, x_j) 是奇置换．

长度 n 的每个圈可以表成 $n-1$ 个对换的乘积，这是因为 $(x_1, x_2, \cdots, x_n) = (x_1, x_2)(x_1, x_3)\cdots(x_1, x_n)$．因而(定理 5.1.1) 每个有限置换都能表成对换的乘积．偶数个对换的乘积是偶置换，奇数个对换的乘积是奇置换．因此，即使一个置换可以用不同方式表成对换的乘积，乘积中对换的个数的奇偶总是相同的．

定理 5.4.2. $A_n(n \geqslant 3)$，是 $n-2$ 重传递的．

证明．设 $y_1, \cdots, y_{n-2}, y_{n-1}, y_n$是$x_1, \cdots, x_{n-2}, x_{n-1}, x_n$ 的任意排列．那么如果

$$u = \begin{pmatrix} x_1, & \cdots, & x_{n-2}, & x_{n-1}, & x_n \\ y_1, & \cdots, & y_{n-2}, & y_{n-1}, & y_n \end{pmatrix},$$

和

$$v = \begin{pmatrix} x_1, & \cdots, & x_{n-2}, & x_{n-1}, & x_n \\ y_1, & \cdots, & y_{n-2}, & y_n, & y_{n-1} \end{pmatrix},$$

则我们有 $v = u \cdot (y_{n-1}, y_n)$，因而 u 和 v 中一个是偶置换，

另一个是奇置换. 因此 A_n 是 $n-2$ 重传递的而不是 n 重传递的，它显然不是 $n-1$ 重传递的，否则还将是 n 重传递的.

在具有 ω 个元素的无限集合的置换群内，我们可以定义交替群 A_ω 由这样的置换组成，它们可以表成偶数个对换的乘积. A_ω 是在这样一个群 H_ω 内的指数为 2 的子群，群 H_ω 由只变动有限个元素的置换组成. 根据定理 5.1.3，H_ω 是 S_ω 的正规子群，A_ω 是 S_ω 的正规子群，它在 H_ω 内的指数是 2 .

定理 5.4.3. 除 $n=4$ 外，对于任何有限的或无限的 n，A_n 是单纯群.

A_2 是单位元素. A_3 是 3 阶循环群，所以是单纯的. 群 A_4 必须单独处理. 我们不妨假定至少有 5 个元素.

引理 5.4.1. $A_n(n \geqslant 3)$ 由所有长度为 3 的圈 (a, b, c) 生成.

证明. A_n 自然是由所有作为两个对换的乘积的元素生成. 如果这两个对换是相同的，则乘积是 1 . 如果它们有一个公共元素，例如 (a, b) 和 (a, c)，则我们有 $(a, b)(a,c)=(a, b, c)$. 如果它们没有公共元素，则$(a,b)(c,d)=(a,b)\cdot(a, c)(c, a)(c, d)=(a, b, c)(c, a, d)$. 引理得到证明.

我们要来证明，包含在 $A_n(n \geqslant 5)$ 内的大于单位元素的正规子群 G 必定包含所有长度为 3 的圈，因而必定等于 A_n. 这要通过处理一系列的情形来确立. 注意因为 $G \subseteq A_n$，G 的每个元素可以表成有限个有限圈的乘积.

情形 1. G 包含长度为 3 的圈 (a, b, c).

这时长度为 3 的任何别的圈 (x, y, z) 与 (a, b, c) 同属于某个 r 个文字的交替群 A_r，这里我们可以取 $r \geqslant 5$. 因为 A_r 是 $r-2 \geqslant 3$ 重传递的，所以 (a, b, c) 和 (x, y, z) 在 A_r 内是共轭的，当然在 A_n 内更是如此. 但是 G 作为正规群必须包

含 (a, b, c) 在 A_n 内的所有共轭者，因而它包含所有长度为 3 的圈. 于是根据引理 5.4.1，$G = A_n$.

情形 2. G 包含具有长度 $s \geqslant 4$ 的圈的元素g.

记

$$g = (a_1, a_2, \cdots, a_r)\cdots(c_1, c_2, \cdots, c_{s-3}, c_{s-2}, c_{s-1}, c_s).$$

这时 $t = (c_{s-2}, c_{s-1}, c_s) \in A_n$，而且

$$t^{-1}gt = (a_1, a_2, \cdots, a_r)\cdots(c_1, c_2, \cdots, c_{s-3}, c_{s-1}, c_s, c_{s-2}).$$

但是 $gt^{-1}g^{-1}t = (c_{s-3}, c_s, c_{s-2})$ 属于 G，因为 G 是正规的. 因而我们把情形 2 化成情形 1.

现在让我们来讨论圈的长度不大于 3 的情形.

情形 3. 某个 $g \in G$ 具有两个或更多的长度为 3 的圈.

$$g = (a^1, a_2, a_3)(b_1, b_2, b_3)\cdots(c_1, \cdots, c_r).$$

取 $t = (a_3, b_1, b_2) \in A_n$. 于是

$$h = t^{-1}gt = (a_1, a_2, b_1)(b_2, a_3, b_3)\cdots(c_1, \cdots, c_r) \in G,$$

而且
$$gh^{-1} = (a_2, b_2, a_3, b_1, b_3) \in G,$$

它就化成情形 2.

情形 4. 某个 $g \in G$ 有一个或更多的长度为 3 的圈，而且它的其余的圈的长度是 2.

$$g = (x_1, x_2)(y_1, y_2)\cdots(z_1, z_2)(a, b, c)\cdots(d, e, f).$$

这时

$$g^2 = (a, c, b)\cdots(d, f, e) \in G.$$

这就化成情形 1 或情形 3.

情形 5. 某个 $g \in G$ 只包含长度为 2 的圈而且它们的个数至少是 4.

$$g = (x, y)(z, u)\cdots(a, b)(c, d) \in G.$$

取 $t = (y, a)(b, c) \in A_n$. 于是

$$h = t^{-1}gt = (x, a)(z, u)\cdots(y, c)(b, d) \in G.$$

$$gh = (x, c, b)(y, a, d) \in G.$$

这就化成情形 3.

情形 6. $g\in G$ 只包含两个长度为 2 的圈

$$g=(a, b)(c, d)\in G.$$

这时因为我们假定 $n\geqslant 5$，存在着被置换的集合的文字 $e, e\neq a, b, c, d$. 于是

$$t=(a, b, e)\in A_n,$$
$$h=t^{-1}gt=(b, e)(c, d)\in G,$$
$$gh=(a, e, b)\in G.$$

这就化成情形 1.

1, 2, 3, 4 上的交替群 A_4 包含一个 4 阶正规子群，它的元素是 (1)，(12)(34)，(13)(24) 和 (14)(23).

5.5. 不传递群．次直积

给了不传递的置换群 G. 设 $S_i(x_{i_1}, \cdots)$ ($i\in I$ 是一个指标集)是它的各个传递区域. 如果我们只考虑 G 对集合 S_i 的文字的作用，则集合 S_i 的这些置换本身组成一个群 G_i. 对于每个 $i\in I$，G 的元素 g 决定一个 $g_i\in G_i$，那就是由 g 产生的 S_i 的文字的置换. 然后我们可以写出

$$g=\prod_i g_i, \tag{5.5.1}$$

即把 g 看作 G_i 的笛卡儿乘积的一个元素，因为在 G 内群的运算与在笛卡儿乘积 $\prod_i G_i$ 内的相合. 因此不传递群可以看作传递群的笛卡儿乘积的一个子群. 这时我们说群 G 是群 G_i 的次直积. 更清楚地说，群 G 叫做群 G_i 的次直积，假如(1) G 是 G_i 的笛卡儿乘积的一个子群；(2) 对于每个 $g_j\in G_j$，至少存在一个 $g\in G$，它以 g_j 作为它的第 j 个分量. 这里第二个条件要求群 G_i 的全体元素确实在 G 的这个表示里出现.

如果在次直积 $G\subseteq\prod\limits_i G_i$ 中所有分量 g_i 可以独立地出现，则 G 是整个笛卡儿乘积. 一般地这并不成立，下面的定理指出在次直积的分量之间可能存在什么样的相关性. 设 G_i 和 G_j 是两个分量，也可以是由两个不相交的分量组决定的群：G_i, $i\in I_1$, G_j, $j\in I_2$, $I_1\cap I_2=0$. 舍弃 G_i 和 G_j 以外的分量时，G 的元素决定一个群 G^*，它是 G_i 和 G_j 的次直积. 我们可以把分量 G_i 和 G_j 在 G 内的相互关系，通过所导出的 G_i 和 G_j 的次直积 G^* 来描述.

定理 5.5.1. 设 G^* 是 G_i 和 G_j 的次直积，H_{ij} 和 H_{ji} 分别是 G_i 和 G_j 的这样的子群，当它们的元素作为一个因子出现在 G^* 内时，另一个因子是单位元素. 那么 H_{ij} 是 G_i 的正规子群，H_{ji} 是 G_j 的正规子群，而且存在着商群之间的同构 $G_i/H_{ij}\cong K\cong G_j/H_{ji}$，使得 $(g_1, g_2)(g_1\in G_i, g_2\in G_j)$ 是 G^* 的元素，必要而且只要 g_1 和 g_2 在同态 $G_i\to K$ 和 $G_j\to K$ 下有相同的像.

证明. 如果 $(h, 1)$ 是 G_i 的子群 H_{ij} 的元素，它在 G^* 中以 G_j 的单位元素作为分量，则我们易于验证 H_{ij} 是 G_i 的正规子群. 同理由 G^* 中 $(1, h)$ 型的元素组成的群 H_{ji} 是 G_j 的正规子群. 其次，对于 $g_1\in G_i$，与这个固定的 g_1 同时出现的元素 $g_2\in G_j$ 的集合是 H_{ji} 的一个傍系. 同理，与固定的 g_2 同时出现的 g_1 的集合是 H_{ij} 的一个傍系. 更进一步，如果 (g_1, g_2) 属于 G^*，则形如 $(H_{ij}g_1, H_{ji}g_2)$ 的全体元素属于 G^*，而且没有 G^* 的任何别的元素 (g_1', g_2') 包含这些元素作为分量. 因此对于 G^* 的每个 (g_1, g_2)，在 H_{ij} 在 G_i 内的傍系和 H_{ji} 在 G_j 内的傍系之间决定了一个一一对应 $H_{ij}g_1\rightleftarrows H_{ji}g_2$.

如果 (g_1, g_2) 和 (g_3, g_4) 属于 G^*，则 (g_1g_3, g_2g_4) 也属于 G^*，因而这个对应保持乘积，即必定是在商群 G_i/H_{ij} 和

G_j/H_{ji} 之间的一个同构. 这时如果我们记 $G_i/H_{ij}=K=G_j/H_{ji}$, 则当 (g_1, g_2) 属于 G^* 时,就有 g_1 和 g_2 属于对应的傍系,因而它们在 G_i 和 G_j 的共同同态像 K 里有相同的像 k.

反之, 如果两个群 G_i 和 G_j 分别有正规子群 H_{ij} 和 H_{ji}, 使得 $G_i/H_{ij}=K=G_j/H_{ji}$, 则 $g_1\in G_i$ 和 $g_2\in G_j$ 的全体对子 (g_1, g_2), 使得在同态 $G_i\to K$ 和 $G_j\to K$ 下有 $g_1\to k$ 和 $g_2\to k$ 的,就组成上面所说的次直积 G^*.

5.6. 本 原 群

假定 G 是某些文字上的置换群, $G\neq 1$, 这些文字可以分成互不相交的集合 S_1, $\cdots$, S_m, 使得 G 的每个置换或者把集合 S_i 的文字还变成这些文字, 或者把它们变成另一个集合 S_j 的文字. 除去只有一个集合或者每个集合由单独一个文字组成的显然情形, 我们说上述 G 是非本原的, 而且把集合 S_1, $\cdots$, S_m 叫做非本原区域. 因此不传递群当然是非本原的. 如果 G 不是非本原的, 则我们说 G 是本原的. 因此本原群是这样的传递群, 它所置换的文字不能分成彼此可以交换的真子集.

定理 5.6.1. 设 G 是非本原的传递群. 设 S_1 是一个非本原区域, y_1 是 S_1 的文字. 又 H 是不变 y_1 的子群. 那么 G 中把 S_1 变成自己的置换组成一个真包含于 G 和 H 之间的子群 K, $G\supset K\supset H$. 非本原区域的个数等于指数 $[G:K]$, 而且每个非本原区域都包含 $[K:H]$ 个文字. 反之, 如果 G 是传递群而且 H 是不变 y_1 的子群, 又如果有一个子群 K 使得 $G\supset K\supset H$, 则 G 是非本原的,而且它的一个非本原区域由 K 把 y_1 变成的 $[K:H]$ 个文字组成. 这时有对应于 K 的左傍系的 $[G:K]$ 个非本原区域. 因此一个置换群 G 是本原的,必要而

且只要不变一个固定文字的子群H是极大子群.

证明. 假定G是非本原的传递群. 设$S_1, \cdots, S_m$是G的非本原区域,又设H是不变 S_1 的 y_1 的子群. 那么如果

$$G = H + Hx_1 + \cdots + Hx_n, \tag{5.6.1}$$

则根据定理 5.3.1,我们可以把被G变换的文字$y_1, y_2, \cdots, y_n$看作按下列规则变换的(5.6.1.)中的左傍系Hx_i, $\pi(g): Hx_i \to Hx_ig$ 对于每个$g \in G$. 如果$y_1, y_2, \cdots, y_t$是S_1的文字,则G中把这些文字变成它们自己的置换组成一个子群K. 不变y_1的置换必定把整个 S_1 变到它自身;因此$H \subset K$, 这是真包含式,因为把y_1变成y_2的置换属于K而不属于H. 现在K是在 S_1的文字上传递的. 因此

$$K = H + Hx_2 + \cdots + Hx_t, \tag{5.6.2}$$

这时S_1的文字的个数t是$[K: H]$. 因为S_1并不包含被G变换的全部文字, 所以K是G的真子群. 现在如果S_i是任意的非本原区域,则就有G的置换把y_1变成S_i的文字, 因而整个S_1变成整个S_i,所以S_i的文字数与S_1相同. 其次,在置换$1 + x_i \to Hx_ig$ 下我们还有$Kx_i \to Kx_ig$, 因而非本原区域就是(5.6.1)中的K的左傍系,所以它们的个数是$[G: K]$.

反之,假定G是传递群,它由不变文字y_1的子群H的傍系的置换$Hx_i \to Hx_ig$给定,又假定存在子群K, 使得$G \supset K \supset H$. 那么K的傍系由H的傍系组成, 而且它们形成G的非本原区域组. 因此G是本原的,必要而且只要子群H是极大的.

我们可以提出由本原性的定义和这个定理得出的几个初等的附注. 二重传递群自然是本原的,因为如果S_1是由受二重传递群G变换的文字的一部分组成的集合, 则就有一个置换把S_1的一个文字变成自己而把S_1的另一个文字变成S_1外的文字. 因而S_1不会是非本原性区域. 其次, n次置换群(置换群的次是指它所变换的文字数, 要具有t个文字的非本原

区域，必须 t 是 n 的约数，因为在定理 5.6.1 里有 $n=[G:H]$ 和 $t=[K:H]$. 因此素数次的置换群总是本原的. 然而在 p 群内每个子群都包含在指数 p 的极大子群内，而且后者是正规的(推论 4.2.2). 因此当置换群是 p 群时，它是非本原的，除非它是 p 次的，这时它是 p 阶循环群.

定理 5.6.2. 设 G 是 n 个文字上的本原置换群，H 是 G 的在 m 个文字上传递的子群，它不变其余 $n-m$ 个文字. 那么(1)如果 H 是本原的，则 G 是 $n-m+1$ 重传递的；(2) 在任何情况下 G 是二重传递的.

证明. H 在 G 所作用的 n 个文字的 m 个上是传递的. H 的每个共轭者是在 m 个文字的一个集合上传递的，而且因为 G 是传递的，每个文字总要在这些集合的一个中出现. 如果这些集合或是不相交的，或是相重的，则它们就将是 G 的非本原区域. 因此存在 H 的共轭者，它变动 H 所变动的若干文字但不是全部文字. 设 H' 是与 H 变动最大个数相同文字的共轭者的一个. 我们记

$$H:(a_1,\cdots,a_r,c_1,\cdots,c_s); \tag{5.6.3}$$
$$H':(b_1,\cdots,b_r,c_1,\cdots,c_s),\ r+s=m.$$

这里我们认为这些 c 是被 H 和 H' 所共同变动的，群 H 还变动 r 个 a_i，群 H' 还变动 r 个 b_i. 我们来证明当 H 是本原群时有 $r=1$，又如果 H 是非本原的而且 $r>1$，则 $a_1,\cdots,a_r$ 是 H 的一个非本原区域. 考虑 H' 的元素 h'

$$h'=\begin{pmatrix}b_1,\cdots, & b_u, & b_{u+1},\cdots, & b_r, & c_1,\cdots, & c_{r-u}, & c_{r-u+1},\cdots, & c_s\\ b,\cdots, & b, & c,\cdots, & c, & b,\cdots, & b, & c,\cdots, & c\end{pmatrix}, \tag{5.6.4}$$

这里只表出有 u 个 b 变成 b，若干 b 变成 c，若干 c 变成 b 和若干 c 变成 c. 注意变成 c 和 b 的个数 $r-u$ 必须与变成 b 的 c 的个数相同，因为在 (5.6.4) 中 h' 的第二行必须有

r 个 b. 因此 $h'^{-1}Hh'$ 变动 r 个 a, $r-u$ 个 b 和 $s-r+u$个 c, 因而就与H有 $s+u$ 个共同的变动文字. 于是如果$r>1$ 而且 H' 是本原的，则我们可以取一个 h', 它把某些而不是全部 b 变成它们自己，因而 $1\leqslant u<r$; 因此 $h'^{-1}Hh'$ 与H有 $s+u$个共同的变动文字,它大于 s 而不等于 $r+s=m$. 当H是本原群时，在任何情况下我们必定有 $r=1$. 而当$r=1$时，不管H是不是本原的，$H\cup H'$ 是在 $m+1$ 个文字上二重传递的，因而是本原的. 我们可以取这个群代替H来继续这个步骤直到达到G本身才止,这时逐步得到的是 $m+1$ 个文字上的二重传递群，$m+2$ 个文字上的三重传递群，直到最后得到G是$n-m+1$ 重传递群.

在H是非本原群的情形,这个论证不能适用,但是我们可以加大H和H'的共同变动的文字数s, 直到$b_1,\cdots,b_r$是H'的一个非本原区域而 $a_1,\cdots,a_r$ 是H的一个非本原区域. 其次,$H\cup H'$ 是$s+2r=m+r$ 个文字上的传递群. 因此，如果m小于$n/2$, $m+r$ 就小于 n. 我们可以逐步组成更多文字上的传递子群，直到得到在大于$n/2$ 但小于n 的m个文字上的传递子群H. 在这种情况下,H的任何共轭者H'与H共同变动若干文字. 这时，假定H是在小于n 的最大可能个数文字上传递的. 如果 $s+2r=n$ 和 $r=1$, 则H是在 $n-1$ 个文字上传递的,因而G是二重传递的. 如果不是这种情况，我们达到一个群H, 这里$s+2r=n$而$r\neq 1$. 在这种情形下，那些 a, b 和 c 全都是G所变动的文字. 但是因为G是本原的,所以存在一个置换 g 把 b_1 变成某个 b_i, 但是并不把全体 b 变成它们自己,因而至少有一个 a 或 c 变成 b. 这时H和$g^{-1}Hg$ 都不变 b_i,而它们的并是在比H多的文字上传递的.因而我们最后必定达到在$n-1$ 个文字上传递的子群，所以G是二重传递的.

定理的第二部分确实可以实现．第一章的例 4 指出了这一点，那里的群是在七个文字上传递的，因而是本原的．它有在四个文字 C，E，F，G 上传递的子群，而且它是二重传递的而不是三重传递的．

5.7. 多重传递群

n 个文字上的对称群自然是 n 重传递的，又交替群 A_n（根据 § 5.4 里的附注）是 $n-2$ 重传递的．在进一步探讨多重传递性时我们可以把这些群除外．存在着无限多个三重传递群．但是把交替群和对称群除外后，已知的只有四个四重传递群．那就是分别在 11，12，23 和 24 个文字上的马帖群，其中在 12 和 24 个文字上的群是五重传递的而且分别包含在 11 和 23 个文字上的四重传递群作为不变某个文字的子群．这些很有意思的群曾经是被人们专门研究的对象，但是还不知道这些群是极为例外的呢，还是它们只是无限个四重传递群中的一部分．

属于密勒（G. A. Miller [1]）的定理 5.7.2 给出 n 次群的传递性的一个极限．把这个定理与"贝尔特朗公设"联合起来，可以证明当 $n>12$ 时，n 次群（除 S_n 和 A_n 外）不会是 $t\geqslant 3\sqrt{n}-2$ 的 t 重传递群．贝尔特朗公设（在 1850 年由契比舍夫给出正确的证明）指出对于任何实数 $x\geqslant 7$，在区间 $x/2<p\leqslant x-2$ 里存在着素数 p．对于 n 的某些极特殊的值，密勒定理给出一个好得多的极限．已知的还有其他很好的限制[1]，但是它们的证明太复杂，不是本书所能介绍的．

定理 5.7.1. 设 G 是 n 个文字上的 t 重传递群．设 H 是

1) 派克(E. Parker) 得到一个极限，对于 n 的合适的值，t 的阶与 $\sqrt[3]{n}$ 相同．最好的近似值由维兰德（Wielandt[1]）提出的是 $t<3\log n$．

不变 t 个文字的子群，又 P 是 H 的西罗 p 子群，这里 P 不变 $w \geqslant t$ 个文字．那么 P 在 G 内的正规化子是在由 P 不变的 w 个文字上的 t 重传递群．

证明．设 $a_1, \cdots, a_t$ 和 $b_1, \cdots, b_t$ 是 t 个文字的两个有序集，它们都从 P 所不变的 w 个文字中取出．那么因为 G 是 t 重传递的，存在着 G 的元素 x 把 a_i 变成 b_i，$i = 1, \cdots, t$．于是 $x^{-1}Px$ 不变 $b_1, \cdots, b_t$，因而 P 和 $x^{-1}Px$ 是不变 $b_1, \cdots, b_t$ 的群的西罗子群．根据西罗第二定理，这两个群在不变 $b_1, \cdots, b_t$ 的群内必定是共轭的．因此，对于不变 $b_1, \cdots, b_t$ 的某个 y，我们有 $y^{-1}(x^{-1}Px)y = P$．于是这时 $z = xy$ 把 $a_1, \cdots, a_t$ 变成 $b_1, \cdots, b_t$ 而且 $z^{-1}Pz = P$．因此在 P 的正规化子内存在元素把由 p 不变的 w 个文字中的任意 t 个文字的有序集变成任意别的同类的有序集．因此 P 在 G 内的正规化子在由 P 不变的 w 个文字上是 t 重传递的．定理证明了．

定理 5.7.2. 设整数 $n = kp + r$，这里 $k > 0$，p 是素数而且 $p > k$，$r > k$．除非 $k = 1$，$r = 2$，n 次群除 S_n 或 A_n 外不可能是 $r+1$ 重传递的．

证明．假定 n 次群 G 是 $r+1$ 重传递的．不变前 r 个文字 $1, 2, \cdots, r$ 的子群 H 是在其余 kp 个文字上传递的．因而 H 的阶能被素数 p 整除而且它包含西罗 p 子群 P．H 的不变一个文字的子群在 H 内的指数是 kp，所以它的阶不能被整除 H 的阶的 p 的最大方幂所整除．因而 P 必须改变 H 在其传递的 kp 个文字中的每一个．其次因为 $kp < p^2$，根据假设 P 不能有 p^2 个文字的传递组．由于在 P 的一个传递组中的文字数是 P 的阶的约数，群 P 在 H 所传递的 kp 个文字上必须恰好有 k 个传递组，每个组都包含 p 个文字．（我们已经排除掉每个传递组由单独一个文字组成的可能性．）P 在每个传递组上的作用必定是 p 阶循环群．因而 P 是各在 p 个文字上的 k 个

p 阶循环群的次直积．因此 P 的每个元素都是 p 阶的，而且 P 是阿贝尔群．但是在多数情况下我们不必考虑 P 是哪样的次直积．

设N是 P 在G内的正规化子．根据定理 5.7.1，N在G的前 r 个文字上是对称群 S_r．让我们先讨论 $r \geqslant 5$ 的情形，而且设N的子群 N_1 在前 r 个文字上是交替群 A_r． 根据定理 5.4.3，A_r 是 $r!/2$ 阶的单纯群,而且因为阶是复合数，它不是阿贝尔群． 设 $T_1, \cdots, T_k$ 是 P 的 k 个包含 p 个文字的传递组．如果我们把前 r 个文字上的置换与在 N_1 下彼此变换的传递组 T_i 上的置换结合起来,可以得出 N_1 的一个同态像．这个像是前 r 个文字上的 A_r 和以某种方式变换上述 k 个 T 的群的次直积．但是 k 个文字上的群最多有阶 $k!$，而因为 $k! < r!/2$，所以它不会有商群同构于作为单纯群的 A_r；因而在这个群的商群中能同构于 A_r 的商群的只有单位元素群．于是这个群包含 A_r，而且根据 § 5.5 的结果，组 T_i 是 A_r 和另一个群的直积．这时 A_r 和另一个群的单位元素在 N_1 内的逆像是一个群 N_2，它是在前 r 个文字上的 A_r，而且它把每个传递组 T_i 变成自己．为了分析 N_2，我们必须考虑由 p 个文字的置换 $a = (x_1, \cdots, x_p)$ 生成的循环群的正规化子的本质．因为 $a^p = 1$，所以如果 $b^{-1}ab = a^i$ 和 $c^{-1}ac = a^j$，则 bc 和 cb 都把 a 变成 a^{ij}．因而由把循环群变成自己而得出的自同构组成一个阿贝尔群．（在下一章我们将会知道 p 阶循环群的自同构群是 $p-1$ 阶循环群．）

现在设 u 是文字 $x_1, \cdots, x_p$ 上的与 a 可交换的置换，当它乘上 a 的适当的方幂 a^i 时，可以得到一个与 a 可交换而且不变文字 x_1 的元素 $v = ua^i$．但是因为 $a^{-1}va = v$ 而且 v 不变 x_1，我们容易证明 v 不变 $x_2, \cdots, x_p$，所以 $v = 1$，因而 $u = a^{-i}$．因此，在 P 的 k 个由 p 个文字组成的传递组T_i 中的

任何一个上，N_2都有一个由p个文字的圈的方幂组成的p阶正规子群，N_2对这个子群的商群由p阶群的不同自同构导出的元素组成；这个商群是阿贝尔群．于是这个群的任何商群或者是阿贝尔群，或者有一个商群是阿贝尔群．因此同构于A_r的一个商群的唯一商群是单位元素群．于是，在略去$T_2, \cdots, T_k$后，当把§5.5的结果应用于前r个文字和T_1时，N_2有一个子群，它在前r个文字上是A_r而在T_1的文字上是单位元素群．其次，N_2的这个子群N_3有一个子群N_4，它在前r个文字上是A_r，而在T_1和T_2上都是单位元素群．

这样继续下去，最后我们得到一个子群，它在前r个文字上是A_r，而在其余的文字上是单位元素群．但是A_r包含三个文字的圈(a, b, c)，而且因为G在全部n个文字上至少是5重传递的，这个圈可以变成n个文字中任何三个文字的圈．根据引理5.4.1，这些三元圈生成A_n，而且因为G包含A_n，G或是A_n或是S_n.

以上的论证要求$r \geqslant 5$，因而还要考虑的是$r=3$，$k=1$或2，以及$r=4$，$k=1, 2$或3的情形．我们先讨论P是由元素a生成的循环群而且$k=1$或2的情形．上面指出过，如果$u=(12)(3)\cdots$和$v=(1)(23)\cdots$是P的正规化子N（它在由P不变的前三个或前四个文字上是对称群）的元素，则因为P是循环群，uv和vu都把a变成它的同一个方幂．因此$u^{-1}v^{-1}uv=(1, 2, 3)\cdots$就与$a$可交换．这个元素$w=u^{-1}v^{-1}uv$或者交换两个传递组$T_1$和$T_2$，或者同时把它们变成自己．不管何种情形，当有两个传递组时，$w^2=(1,3,2)\cdots$总不变这两个组．这个元素的阶能被3整除；因而它的某个方幂的阶是3^s，而且在前三个文字上仍然是一个三元圈，它把传递组变成自己而且与a可交换．但是对于a的每个圈，唯一可交换的元素是这个圈的方幂，因而在它不是单位元素

时必须是 p 阶的. 因此，除非 $p=3$，以这种方式与 a 可交换的 3^s 阶元素在前三个文字上是 (1, 2, 3) 或 (1,3, 2) 而在其余的文字上是单位元素. 这时 G 包含一个三元圈而且是三重传递的，因而必须是 A_n 或 S_n. 我们除外的只是 $p=3$，这对应于 $k=1$ 或 2 而且 $r=3$ 或 4，因而 $n=6,7,9,10$. 确切地说，当 $p=3$, $k=1$ 时，P 本身由三元圈生成，结论也就得出了. 这就解决了 $n=6$ 和 7 的情形而留下 $n=9$ 和 10 作为特别情形来讨论. 这时 $k=1$ 的所有情形都已解决，因为在这些情形下 P 显然是循环群. 现在如果 $k=2$ 而且 P 不是循环群，则 P 是两个 p 阶循环群的直积. 于是由于 G 是本原群而且 H 包含一个 p 阶圈，由它生成的子群 H' 当然是本原群. 对 G 和 H' 应用定理 5.6.2，那么 G 必定是 $p+4$ 重或 $p+5$ 重传递的. 于是我们可以利用 $r=p+3$ 或 $p+4$ 和 $k=1$ 的论证来得出 $G=A_n$ 或 S_n.

剩下要考虑的是 $k=3$ 和 $r=4$ 的情形. 首先，如果 P 是循环群，则我们可以像前面那样断定，存在着元素 (1,2,3)(4)… 和 (1) (2, 3, 4)… 以及前四个文字上的所有八个可能的三元圈，它们都与 P 的一个生成元素 a 可交换. 但是它们将会以 (T_1, T_2, T_3) 或 (T_1, T_3, T_2) 的方式循环地变换 a 的三个传递组，而且在八个中至少有两个会以同样的方式变换这些 T. 把这些论证联合起来，我们得到一个形如 (1, 2, 3)(4)… 或 (1, 2) (3, 4)… 的元素，它把 T_1, T_2, T_3 都变成自己. 这时 p 至少是 5，而且与 a 可交换而又把 a 中的圈变成自己的一个这种形式的元素导出不变 a 的 $3p$ 个文字的一个同一形式的元素. 因而在 G 中或有一个三元圈 (1, 2, 3)，或有一个元素 (1, 2)(3, 4)，而且由于四重传递性，还有元素 (1, 2)(3, 5) 和三元圈 (3, 4, 5). 因此 G 包含 A_n，即是 A_n 或 S_n. 另一方面，如果 P 包含 p 个文字的单独一个圈，则可

以应用定理 5. 6. 2，这时G是$2p+4$重或$2p+5$重传递的，因而G又是A_n或S_n.

最后还必须考虑P既不是循环群又不包含p元圈的可能情形．在这种情形下P必须是p^2阶的．我们可以取两个元素$a=(x_1, x_2, \cdots, x_p)(y_1, y_2, \cdots, y_p)$和$b=(y_1, y_2, \cdots, y_p)\cdot(z_1, z_2, \cdots, z_p)$作为$P$的基底，这里我们取$a$和$b$在$y_i$上的圈相同．于是唯有$ab^{-1}$和它的方幂是$P$中不变由$y_i$组成的传递组$T_2$的元素．现在在$P$的正规化子中可以找到有形如$(1,2,3,4)\cdots$的一个元素，它或者不变全部三个传递组，或者交换其中的两个而不变第三个．于是它的平方$u=(1,3)\cdot(2,4)\cdots$不变全部三个传递组．因此u把a，b和ab^{-1}的每一个变成自己的某个方幂，因而把a和b同时变成它们的同一个方幂(设是i次方幂，因而P的每个元素都变成它的i次方幂)．这样一个自同构必定与P的任何其他自同构可交换，特别说来也与由元素$w=(1)(2)(34)\cdots$导出的自同构可交换．因此$v=w^{-1}uw=(1,2)(3,4)\cdots$也把$P$的每个元素变成它的$i$次方幂，因而它自然不变$P$的传递组．但是现在$uv^{-1}=(1,4)(2,3)\cdots$与$P$中每个不变这些传递组的元素可交换．这说明$G$中存在元素$(1,4)(2,3)$，而且因为$G$是多于四个文字上的四重传递群，所以$G$仍然是$A_n$或$S_n$.

5.8. 约当定理

在 1872 年约当 (Jordan [2]) 证明了，只有单位元素群才不变四个文字的有限四重传递群必定是下列群中的一个：四个或五个文字上的对称群，六个文字的交替群，或十一个文字的马帖群.

关于四重传递群的约当定理在这里以两种方式来推广.

其一是：文字的个数不假定为有限的；其二是：把不变四个元素的子群只包含单位元素换成它是奇数阶的有限群．得到的结论就其主要方面说与约当定理相同，满足这些假设的唯一外加的群是七个文字的交替群．

这个定理是这样的：

定理 5.8.1. 如果群 G 是在一组文字（有限个或无限个）上的四重传递群，它有一个不变四个文字的子群 H 是奇数阶的有限群，则 G 必定是下列群中的一个：S_4，S_5，A_6，A_7 或 11 个文字上的马帖群．

情形 1. G 在不多于七个文字上．四个或五个文字上的四重传递群必定是对称群．在六个文字上，它的阶至少是 $6\cdot5\cdot4\cdot3$，因而它是 A_6 或 S_6．在七个文字上，它在 S_7 内的指数最多是 6．因为 S_7 不包含指数为 3 或 6 的子群，所以它只可能是 A_7 和 S_7．在 S_6 和 S_7 中都存在 2 阶元素不变至少四个的文字，所以这两个群不满足我们的假设．

为了处理 G 是在多于七个的文字上的群的情形，我们先证明一个引理．

引理 5.8.1. 在满足关系

$$a^2=1,\ b^2=1,\ (ab)^s=1$$

的群里，元素 a 和 b 生成 $2s$ 阶的二面体群．如果 $s=2t-1$ 是奇数，则 $y=ab$ 的一个方幂把 a 变成 b．如果 $s=2r$ 是偶数，则 a 和 b 都与 y^r 可交换．

证明. 取 $y=ab$，我们有

$$a^2=1,\ y^s=1,\ b=ay=y^{-1}a.$$

如果 $s=2t-1$，则

$$y^{-t}ay^t=ay^{2t}=b.$$

如果 $s=2r$，则

$$ay^r=y^{-r}a=y^ra.$$

从这里开始，G总表示（像在定理 5.8.1 中那样）在七个以上的文字上的四重传递群，而H则表示不变四个文字的奇数m阶子群.

引理 5.8.2. 设群G包含 2 阶元素，而且所有 2 阶元素都是共轭的．那么或者（1）每个 2 阶元素不变两个文字，或者（2）每个 2 阶元素不变三个文字.

证明. 由于四重传递性，G包含一个元素

$$g=(12)(34)\cdots.$$

这时 g^2 不变 1，2，3，4，因而属于H而且有奇数阶 m_1．于是

$$x=g^{m_1}=(12)(34)\cdots,$$

而有 $x^2=1$．因为H是奇数阶的，所以G的任何 2 阶元素 u 最多不变三个文字，因而至少变动四个文字．设

$$u=(ab)(cd)\cdots,$$

那么就有 u 的共轭者

$$v=w^{-1}uw=(12)(34)\cdots.$$

于是或者 $v=x$，或者 vx 不变四个文字而且是奇数阶的，因而根据引理 5.8.1，v 和 x 是共轭的．因此所有 2 阶元素都是共轭的．另一方面，在G内存在一个元素 $z=(1)(2)(34)\cdots$，而且 z 或 z 的一个奇次方幂是至少不变两个文字的 2 阶元素．因此每个 2 阶元素不变两个或三个文字，因为它们至少不变两个文字而且不能不变四个文字.

情形 2. G 在多于七个文字上．设

$$a_1=(1)(2)(34)\cdots$$

是一个 2 阶元素，而且

$$b=(12)(34)\cdots$$

是另一个 2 阶元素．那么 $f=a_1b=(12)(3)(4)\cdots$ 是偶数阶的，而且 f^2 是奇数 m_1 阶的．因此 $f^{m_1}=a_3$ 是 2 阶的，而且根据引理 5.8.1，它与 a_1 可交换．于是在G内有了三个可交换

的 2 阶元素 a_1, a_2 和 a_3, 这里 $a_2 = a_1a_3$.

$$\begin{aligned} a_1 &= (1)(2)(34)\cdots, \\ a_2 &= (12)(34)\cdots, \\ a_3 &= (12)(3)(4)\cdots. \end{aligned} \tag{5.8.1}$$

现在 a_2 作为 2 阶元素，它或者不变两个文字 5 和 6，或者不变三个文字 5, 6 和 7. 因为 a_1 与 a_2 可交换，所以 a_1 把这些文字变到它们自身. 但是 a_1 不变 1 和 2，因而最多再不变一个文字. 因此我们有

$$\begin{aligned} a_1&=(1)(2)(34)(56)\cdots, & a_1&=(1)(2)(34)(56)(7)\cdots, \\ a_2&=(12)(34)(5)(6)\cdots, \text{或} & a_2&=(12)(34)(5)(6)(7)\cdots, \\ a_3&=(12)(3)(4)(56)\cdots; & a_3&=(12)(3)(4)(56)(7)\cdots. \end{aligned} \tag{5.8.2}$$

当 2 阶元素全都不变两个文字时出现第一种情形；全都不变三个文字时出现第二种情形. (5.8.2)的元素 a_1, a_2, a_3 和单位元素组成一个四阶群 V. 其他的文字将以四个一组作为 V 的传递组而出现:

$$\begin{aligned} a_1 &= (1)(2)(34)(56)(7)(hi)(jk)\cdots, \\ a_2 &= (12)(34)(5)(6)(7)(hj)(ik)\cdots, \\ a_3 &= (12)(3)(4)(56)(7)(hk)(ij)\cdots. \end{aligned} \tag{5.8.3}$$

这里应该理解为 7 可以不出现.

把 h, i, j, k 变到它们自身的子群 K 的阶是 $24m$, 而且不变这些文字的 m 阶子群 $H = H(h, i, j, k)$ 在 K 内是正规的. 还应该有一个子群 U, $K \supset U \supset H$, 在 U 中 h, i, j, k 以下列方式变换:

$$\begin{array}{c} (h) \\ (hi)(jk) \\ (hj)(ik) \\ (hk)(ij) \end{array} \tag{5.8.4}$$

$$(hijk)$$
$$(hkij)$$
$$(hi)(j)(k)$$
$$(h)(i)(jk).$$

因为U是$8m$阶的，所以U的一个西罗子群是8阶的．以特定方式把h，i，j，k变到它们自身的元素组成H在U内的一个傍系．因为H在U内是正规的，U内的8阶子群在H的每个傍系中各有一个元素，因而它同构于U/H，因此适宜于用这些文字上的置换来表示．V包含在U内的一个8阶的西罗子群中．这就得出

$$\begin{aligned}
a_1 &= (1)(2)(34)(56)(7)(hi)(jk)\cdots,\\
a_2 &= (12)(34)(5)(6)(7)(hj)(ik)\cdots,\\
a_3 &= (12)(3)(4)(56)(7)(hk)(ij)\cdots,\\
u &= (1)(2)(3546)(7)(hjik)\cdots,\\
a_1u &= (1)(2)(3645)(7)(hkij)\cdots,\\
a_2u &= (12)(36)(45)(7)(hi)(j)(k)\cdots,\\
a_3u &= (12)(35)(46)(7)(h)(i)(jk)\cdots,
\end{aligned} \tag{5.8.5}$$

或者是交换5和6而得到的同样一些置换．后四个元素变换1，…，7的方式由下列关系决定：

$$u^2 = a_1,\ u^{-1}a_2u = a_3,\ (a_2u)^2 = 1.$$

这时u属于V的正规化，因而它不变V所不变的唯一文字7（如果7出现的话）．其次，u必须把a_3的不变文字变成a_2的不变文字，因而

$$u = \begin{pmatrix}3, & 4, & \cdots\\ 5, & 6, & \cdots\end{pmatrix} \quad 或 \quad u = \begin{pmatrix}3, & 4, & \cdots\\ 6, & 5, & \cdots\end{pmatrix};$$

但是还有$u^2 = a_1$，因而

$$u = (3546)\cdots \quad 或 \quad u = (3645)\cdots.$$

最后，u 必须不变 1 和 2 或者把它们交换．但是如果 u 交换 1 和 2，则 a_2u 是 2 阶的而且不变文字 1，2，j，k．因此

$$u=(1)(2)(3546)\cdots \quad 或 \quad u=(1)(2)(3645)\cdots,$$

其他可以接着得出．

V 的类似于 h，i，j，k 的每个别的传递组，产生类似于 (5.8.5) 那样的一个群 S．在每一个这种群内，元素

$$(12)(36)(45)\cdots \quad 和 \quad (12)(35)(46)\cdots$$

不变传递组的两个文字．因为 2 阶元素不能不变四个文字，所以每个传递组对应于一个以 (12) (36) (45) 的方式变换前六个文字的不同的元素．但是最多存在 m 个以这种方式作用于前六个文字的元素．因此如果存在 t 个这种传递组，则 $t\leqslant m$ 是有限的，而且 G 是在 $n=4t+6$ 或 $4t+7$ 个文字上的群．如果 G 是在 10 个或 11 个文字上的群，则我们有 $t=1$．

不存在十个文字上的四重传递群（当然把 A_{10} 和 S_{10} 除外），因为根据定理 5.7.2，长度为 7 的圈的正规化子在其余三个文字上是 S_3；这个正规化子是 S_3 和这个七元圈的文字上的正规化子的次直积，所以它使一个三元圈与单位元素成对．因此 G 包含一个三元圈，而由于它是四重传递的，它包含全部三元圈；因此 G 包含 A_{10}．

在11个文字上，G 的阶是 $11\cdot10\cdot9\cdot8m$，而且即使未假定 m 是奇数，只要讨论不变四个文字的西罗子群的正规化子，就能证明必须有 $m=1$．不变三个文字的 8 阶子群包含单独一个 2 阶元素，因而它是循环群或四元数群．只有四个自同构的循环群不能有一个正规化子是在其余三个文字上三重传递的，因为这样 G 就将包含一个三元圈．因此不变三个文字的子群必须是四元数群 Q．于是 G 就是 Q 的传递的扩张，于是运用荷辽克 (T. C. Holyoke [1])的方 法就能从 Q 构造出不仅是 11 个文字上的四重传递的马帖群， 而且还有

12 个文字上的五重传递群.

我们现在来证明，$t>1$ 与H是奇数阶的假设矛盾，因而就完成了我们的定理的证明. 如果 w, x, y, z 是V的另一个传递组，则我们从 (5.8.5) 有

$$a_2u=(12)(36)(45)(7)(hi)(j)(k)\cdots,$$

而且还有另一个元素

$$a_2u'=(12)(36)(45)(7)(wx)(y)(z)\cdots.$$

这两个元素中每一个都与 a_1 可交换而且把 a_2 和 a_3 变成 a_2. 它们的乘积是不变前六个（或七个）文字的一个元素 q, 因而它是奇数阶的. 再有，q 属于V的中心化子. 根据引理5.8.1, q 的一个方幂把 a_2u 变成 a_2u', 因而把 a_2u 不变的文字 j 和 k 变成 a_2u' 不变的文字 y 和 z. 因为这个元素属于 V 的中心化子，它必须把整个传递组 $hijk$ 变成 $wxyz$. 因此在G内存在不变前六个（或七个）文字的群 C, 它属于V的中心化子而且在V的其余 t 个传递组上是传递的. 把V的一个传递组变到自身的、C的一个奇数阶元素，必定不变全部四个文字. 因此C的传递组是(1), (2), (3), (4), (5), (6), (7), T_h, T_i, T_j, T_k, 后四个组各包含 t 个文字，而且 h, i, j, k 属于C的不同的传递组.

设 p 是整除 t 的一个素数.（这里我们用到假设$t>1$.）设P是C的对应的西罗子群. 那么P变动C所变动的全部 $4t$ 个文字，因为C的不变一个文字的子群的指数 $t\equiv 0\ (\bmod p)$, 因而不能包含这样一个西罗子群. 现在设H是包含P的不变1, 2, 3, 4 的子群，P_1是H的西罗子群. 那么P_1变动C的 $4t$ 个文字而不变其他，除非我们可能有情形

$$p=3,\ t=3^w,\ n=4t+7,$$

这里P_1可以是在 $4t+3$ 个文字上的群. 这个可能性在以后再讨论. 对于P_1在 $4t$ 个文字上的情形，根据定理 5.7.2，群

$N_G(P_1)$ 是在前六个或七个文字上四重传递的，因而包含着这些文字上的 A_6 或 A_7. 但是把前六个（或七个）文字变到它们自身的子群也包含 (5.8.5) 的元素 u，它不属于这些文字上的交替群. 于是在 G 内我们有了在前六个或七个文字上的完全对称群，因此有某个元素不变前四个文字而且交换第五个和第六个文字. 这与 H 有奇数阶的假设矛盾. 最后来讨论可能情形

$$t = 3^w, \quad n = 4t + 7.$$

这时 P_1 既变动 5,6,7，也变动 P 的 $4t$ 个文字. 如果 $w > 1$，则当然 5，6，7 是 P_1 的传递组，而且在 G 内存在一个元素

$$z = (1)(2)(3)(4)(567)\cdots.$$

如果 $w = 1$，则 P 是 3 阶的，而且（即使在 P_1 内，5，6，7 与 P 的传递组 8，9，10 和 11，12，13 同在一个传递组内）因为存在一个元素(5)(6)(7)(8，9，10)(11，12，13)，所以也存在如同 z 那样的一个不变 8，9，10 的元素. 但是对于 $z = (1)(2)(3)(4)(567)\cdots$ 和 (5.8.5) 中的 u，我们有

$$(zu)^3 = (1)(2)(35)(4)(6)(7)\cdots,$$

这与 H 是不变四个文字的奇数阶子群相矛盾.

设 G 是 11 个文字上的四重传递群，不包括 S_{11} 和 A_{11}. 如果 G 包含形状为 (a,b)，$(a,b)(c,d)$，(a,b,c) 中之一的元素，则由于四重传递性，G 包含全体这种元素因而必须是 A_{11} 或 S_{11}. 如果 G 包含一个五元圈或七元圈，则这样一个元素生成的群是在它所变动的文字上传递的和本原的. 在这种情况下，根据定理 5.6.2 和 5.7.1，G 必定是 S_{11} 或 A_{11}. 除掉这些例外情形，有一个不变四个元素的子群 $V = V_{1234}$ 的阶整除 $2^4 3^2$. 如果 V 不是单位元素群，则 V 必定有一个西罗 2 群或西罗 3 群. 由于排除了例外情形，任何这样的西罗子群 P 必须变动恰好六个文字. 根据定理 5.7.2，P 的正规化子在余下的五个

文字上是四重传递的，而且因为P的传递组是两组三个文字的，或一组四个和一组两个文字的，或三组两个文字的，就将得出G包含一个五元圈，这是已经除外的情形．因而剩下的唯一可能情形是：有一个不变四个元素的子群V是单位元素群而且G的阶是 $11\cdot 10\cdot 9\cdot 8$．

不变三个文字（例如 9，10，11）的子群W在其余八个文字上是正则的和传递的，因而它是五个不同的 8 阶群之一的正则表示．W要包含一个 2 阶元素，例如$x=(1,2)(3,4)\cdot(5,6)(7,8)(9)(10)(11)$．在不变两个文字 10 和 11 的子群$H$内有$W$的九个共轭者，每一个都不变另一个文字．如果两个不同的 2 阶元素包含同一个对换例如(i,j)，则它们的乘积是最多变动七个文字的不是单位元素的元素．这是不可能的．但是每个 2 阶元素包含着四个对换，而且一共只有$1,\cdots,9$的$9\cdot 8/2=36$个可能的对换．因此W只包含一个 2 阶元素，因而必定是 8 阶循环群或四元数群．但是如果W是循环群，则它的正规化子包含一个 3 阶元素，这只能是圈$(9,10,11)$，然而这是不可能的．因此W必定是四元数群Q．

不变 10 和 11 的子群H是 72 阶的而且包含九个四元数子群，其中任何两个的交都是单位元素群．单位元素和其余八个元素组成一个 9 阶子群U，它在H内是正规的．U的八个不是单位元素的元素在Q下是共轭的，因而U必定是初等阿贝尔群．

根据这个结论我们容易构造H，它是唯一的，最多相差一个置换同构．U可以由下列元素生成：

$$u=(123)(456)(789)(10)(11),$$

$$v=(147)(258)(369)(10)(11).$$

$H=QU$，这里Q是由下列元素生成的四元数群：

$$a=(1)(2437)(5698)(10)(11),$$

$$b=(1)(2539)(4876)(10)(11),$$

而且

$$a^2=b^2=(1)(23)(47)(59)(68)(10)(11).$$

不变 11 的子群 K 由 H 和 a^2 的一个共轭者 x 生成，x 不变 2 和 11 而且交换 1 和 10. 因为 G 是四重传递的，这样一个元素必定存在. x 显然属于 Q 的正规化子. 把 x 添加在 H 上必定不会产生一个不变四个文字而又不是单位元素的元素. 可能的 x 只是

$$x_1=(1,10)(2)(3)(11)(4,5)(6,8)(7,9),$$

$$x_2=(1,10)(2)(3)(11)(4,6)(5,9)(7,8),$$

$$x_3=(1,10)(2)(3)(11)(4,7)(5,6)(8,9).$$

元素 $(4,5,6)(7,8,9)$ 把 H 变成自身而且把这三个元素互相交换，在相差一个置换同构下，我们可以把这三个元素中任何一个添加到 H 上. 设 K 是把 x_1 添加到 H 上而得到的群. 那么 G 就由 K 添加 a^2 的一个共轭者 y 而得到，这里 y 交换 1 和 11 而且不变 2 和 10. 这时 y 同时属于 Q 的正规化子和不变 1 和 11 的子群的正规化子. 可能的 y 只是

$$y_1=(1,11)(2)(3)(10)(4,6)(5,9)(7,8),$$

$$y_2=(1,11)(2)(3)(10)(4,7)(5,6)(8,9).$$

这时元素 $(4,9)(5,7)(6,8)$ 属于 K 的正规化子而且它使 y_1 和 y_2 交换. 因此，最多相差一个置换同构，我们可以假定 G 从把 y_1 添加到 K 上而得到. $G=\{H,x_1,y_1\}$. 严格地说，我们证明了的只是，如果存在一个 11 个文字上的四重传递群不是 A_{11} 或 S_{11}，则它置换同构于 G. 验证 G 具有这些性质是习题 4 所要求的. 大家把 G 叫做 11 个文字上的马帖群 M_{11}. 值得指出以下的重要事实：如果我们把 M_{11} 看做 12 个文字上不变 12 的置换群，而且我们取群 $M_{12}=\{M_{11},z\}$，这里

$$z=(1,12)(2)(3)(10)(11)(4,7)(5,6)(8,9),$$

则我们发现 M_{12} 是12 · 11 · 10 · 9 · 8 阶的五重传递群，而且 M_{11} 是不变 12 的子群.

根据类似于在构造 M_{11} 时所用的论证，我们可以证明在小于35个文字上的四重传递群(不是交替群或对称群)，只有 M_{11}，M_{12} 和在 23 和24个文字上的马帖群 M_{23} 和 M_{24}. 这时如果取

$$
\begin{aligned}
A &= (0, 1, 2, \cdots, 22), \\
B &= (2, 16, 9, 6, 8)(4, 3, 12, 13, 18) \cdot \\
&\quad (10, 11, 22, 7, 17)(20, 15, 14, 19, 21), \\
C &= (0, 23)(1, 22)(2, 11)(3, 15)(4, 17)(5, 9) \cdot \\
&\quad (6, 19)(7, 13)(8, 20)(10, 16) \cdot \\
&\quad (12, 21)(18, 14),
\end{aligned}
$$

则 $M_{23} = \{A, B\}$ 和 $M_{24} = \{A, B, C\}$. M_{23} 是 23 · 22 · 21 · 19 · 16 · 3 阶的 23 次的四重传递群，M_{24} 是五重传递群，而且 M_{23} 是 M_{24} 的不变 23 的子群.

5.9. 织积. 对称群的西罗子群

设 G 和 H 分别是在集合 A 和 B 上的置换群. 我们以下列方式定义 G 乘 H 的织积，记做 $G \wr H$：$G \wr H$ 是在 $A \times B$ 上的全体下列类型的置换 θ 的群：

$$(a, b)\theta = (a\gamma_b, b_\eta), \ a \in A, b \in B, \tag{5.9.1}$$

这里对于每个 $b \in B$，γ_b 是 G 在 A 上的一个置换，但是对于不同的 b，置换 γ_b 的选取是独立的. 置换 η 是 H 在 B 上的置换. $\eta = 1$ 时的置换 θ 组成一个正规子群 G^*，它同构于 n 个 G 的直积，这里 n 是集合 B 中的文字的个数. 商群 G/G^* 同构于 H. 全体 $\gamma_b = 1$ 的置换 θ 组成一个子群同构于 H，这个子群的元素可以取作 G^* 在 G 内的傍系代表.

织积在下列意义下是可结合的：如果K是在集合C上的第三个置换群，则$(G \wr H) \wr K$和$G \wr (H \wr K)$是同构的，而且如果我们把集合$(A \times B) \times C$和$A \times (B \times C)$与$A \times B \times C$等同起来，则它们还是重合的.

对称群S_n的西罗子群易于用织积来构造. 什么是整除$n!$的p的最高方幂？$n!$中被p整除的因子是$p, 2p, 3p, \cdots, kp$，这里$k = [n/p]$是不大于n/p的最大整数. 因此$n!$能被p^k和整除$k!$的p的方幂的乘积整除. 由于$[k/p] = [n/p^2]$，继续同样的论证，可以得出整除$n!$的p的最大方幂是p^M，这里

$$M = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots.$$

如果我们把n表示成p进位数

$$n = a_0 p^u + a_1 p^{u-1} + \cdots + a_{u-1} p + a_u, \qquad (5.9.2)$$

这里每个a_i的范围是$0 \leqslant a_i \leqslant p-1$，则我们有

$$M = a_0(p^{u-1} + p^{u-2} + \cdots + p + 1) + a_1(p^{u-2} + \cdots + p + 1) + \cdots + a_{u-1}. \qquad (5.9.3)$$

特别地，在p^r个文字上的对称群的西罗子群的阶是p^{N_r}，这里$N_r = p^{r-1} + p^{r-2} + \cdots + 1$. 因此，构造了在$p, p^2, \cdots, p^u$个文字上的对称群的西罗子群以后，我们易于构造在$n$个文字上的对称群的一个西罗子群，这里$n$由(5.9.2)给出. 我们把$n$个文字分割成$a_0$组$p^u$个文字，$a_1$组$p^{u-1}$个文字，$\cdots, a_{u-1}$组$p$个文字和$a_u$组单独一个文字. 那么如果我们在每个组内构造了适当的西罗子群而且取它们的直积，我们就将有一个p^M阶的群P，这里M由(5.9.3)给出. 因此P是S_n的一个西罗子群.

在$1, 2, \cdots, p$上的S_p的西罗子群是p阶的，因而有一个西罗子群是由$a_1 = (1, 2, \cdots, p)$生成的p阶循环群. 在

1, 2, $\cdots$, p^2 上的 S_{p^2} 有一个子群是由 $a_1=(1,2,\cdots,p)$, $a_2=(p+1,p+2,\cdots,2p)$, $\cdots$, $a_p=(p^2-p+1,\cdots,p^2)$ 生成的循环群的直积，如果我们再取一个 p 阶元素 $b=(1,p+1,2p+1,\cdots,p^2-p+1)(2,p+2,\cdots)\cdots(p,2p,\cdots,p^2)$，则 $b^{-1}a_ib=a_{i+1}'$，这里指标是对模 p 取的. 因此 b 和这些 a 生成一个 p^{p+1} 阶群 P_2，它是由 b 生成的循环群和由 a_1 生成的循环群的织积. 这时 P_2 是 S_{p^2} 的西罗子群.一般地说，设 P_r 是在 1, $\cdots$, p^r 上的 S_{p^r} 的西罗子群. 取文字 1, $\cdots$, p^r, p^r+1, $\cdots$, $2p^r$, $\cdots$, p^{r+1} 作为 $S_{p^{r+1}}$ 的文字. 那么只要取元素

$$c=[1,p^r+1,2p^r+1,\cdots,(p-1)p^r+1]\cdots$$
$$[j,p^r+j,\cdots,(p-1)p^r+j]\cdots,$$

这里 j 取 1 到 p^r 的值，我们就有 $P_{r(i)}=c^{-i}P_rc^i$ 是在文字 ip^r+1, $\cdots$, $(i+1)p^r$ 上的 p^{N_r} 阶群. 由于每个 $P_{r(i)}$, $i=0$, 1, $\cdots$, $p-1$ 变动互不相同的一组文字,由它们生成的群是它们的直积. 这时 c 和 P_r 生成一个 p^{pN_r+1} 阶群. 但是因为 $pN_r+1=p[p^{r-1}+\cdots+(p+1)]+1=N_{r+1}$, 所以 c 和 P_r 生成 P_{r+1}, 它是 p^{r+1} 个文字上的对称群的西罗子群. 设 P_r 作用于文字 1, $\cdots$, p^r 上，而且取 c 为圈 $c=(u_0,u_1,\cdots,u_{p-1})$,则织积 $P_r\wr\{c\}$ 作用于符号 (i,u_j), $i=1$, $\cdots$, p^r, $j=0$, $\cdots$, $p-1$. 如果我们把 (i,u_j) 与 $i+jp^r$ 等同起来，则前面定义的 P_{r+1} 恰好是织积 $P_r\wr\{c\}$. 我们附带看到 P_r 是由 r 个 p 阶元素生成的.

为了说明起见，我们提出 S_8 的一个 2^7 阶的西罗 2 子群，它由下列元素生成:

$$a_1=(1,2),$$
$$b_1=(1,3)(2,4),$$
$$c_1=(1,5)(2,6)(3,7)(4,8).$$

习　　题

1. 设无限群 G 有一个子群 H 是有限指数的，证明存在一个子群 $K\subset H$，这里 K 在 G 内是正规的和有限指数的.（提示：把 G 表示成 H 的傍系上的置换群.）
2. 证明只存在一个 60 阶的单纯群，那就是五个文字上的交替群.
3. 证明 S_4 有两个在六个文字上的传递表示，它们都是一一的但是并不是置换同构的.
4. 给了置换

   $u=(1,2,3)(4,5,6)(7,8,9)$,

   $a=(2,4,3,7)(5,6,9,8)$,

   $b=(2,5,3,9)(4,8,7,6)$,

   $x=(1,10)(4,5)(6,8)(7,9)$,

   $y=(1,11)(4,6)(5,9)(7,8)$,

   $z=(1,12)(4,7)(5,6)(8,9)$.

   证明 $\{u,a,b,x,y\}$ 是 11 次的和 $11\cdot 10\cdot 9\cdot 8$ 阶的四重传递的马帖群 M_{11}，又 $\{M_{11},z\}$ 是五重传递的马帖群 M_{12}，在其中 M_{11} 是不变 12 的子群.
5. 给了置换

   $a=(0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,$
   $16,17,18,19,20,21,22)$,

   $b=(2,16,9,6,8)(3,12,13,18,4)(7,17,10,$
   $11,22)(14,19,21,20,15)$,

   $c=(0,23)(1,22)(2,11)(3,15)(4,17)(5,9)(6,19)\cdot$
   $(7,13)(8,20)(10,16)(12,21)(14,18)$.

   证明 $\{a,b\}$ 是 23 次的和 $23\cdot 22\cdot 21\cdot 20\cdot 16\cdot 3$ 阶的四重传递的马帖群 M_{23}，而且 $M_{24}=\{a,b,c\}$ 是五重传递的马帖群，在其中 M_{23} 是不变 23 的子群.

第六章　自　同　构

6.1. 代数体系的自同构

在 §1.2 里我们说过，任何集合到自身上的全体 1—1 映射组成一个群。一般地说，集合 S 到自身上的保持某些性质 P 的 1—1 映射也组成一个群.

设 A 是某个一般的代数体系，它具有元素集合 $X=\{x\}$ 和运算 f_μ，使得当 $x_1, \cdots, x_n$ 是 A 的元素时，$f_\mu(x_1, \cdots, x_n)=y$ 是 A 的一个元素. 可以有任意多个运算，但是每个运算是有限的 n 个元素的一个单值函数. A 的"定律"或"公理"是包含这些运算的一些关系. 那么对于 X 到自身上的 1—1 映射 $\alpha: X \rightleftarrows X^\alpha$，如果对于每个运算 f_μ 和在给定 f_μ 时对于所有 $x_1, \cdots, x_n$，都有

$$f_\mu(x_1, \cdots, x_n)=y \text{ 蕴涵 } f_\mu(x_1^\alpha, \cdots, x_n^\alpha)=y^\alpha, \quad (6.1.1)$$

则 α 叫做 A 的一个**自同构**. 作为两个自同构的乘积的映射本身是一个自同构，而且对于这种乘积而说，自同构组成一个群. 特别地，群的自同构组成一个群. 在群内只有单独一个二元运算，即乘积运算，这时为了使 1—1 映射 α 成为自同构，只需要从 $ab=c$ 得出 $a^\alpha b^\alpha=c^\alpha$，或更简捷些是 $(ab)^\alpha=a^\alpha b^\alpha$.

代数体系的自同构是群的一个自然来源. 历史上群论是随着代数域的自同构的研究而发展起来的.

6.2. 群的自同构.内自同构

设 $\alpha: x \rightleftarrows x^\alpha$ 是从群 G 到自身上的 1—1 映射，α 是自

同构，必要而且只要从 $ab=c$ 得出 $a^\alpha b^\alpha = c^\alpha$，或更简洁些是

$$(ab)^\alpha = a^\alpha b^\alpha. \tag{6.2.1}$$

单是关系 (6.2.1) 决定的是自同态，在 §2.4 里我们曾经把自同构定义为 1—1 的自同态． 因而群自同态的这两种定义是一致的．

对于固定的 $a\in G$，下列映射 A_a

$$A_a: x \rightleftarrows a^{-1}xa, \text{ 对于所有 } x\in G \tag{6.2.2}$$

确实是一一的， 因为 $axa^{-1} \to a^{-1}(axa^{-1})a = x$． 又因为 $a^{-1}xya = a^{-1}xa \cdot a^{-1}ya$，它还是一个自同构． 由 (6.2.2) 表出的 G 的自同构 A_a 叫做内自同构． G 的不是这种类型的自同构叫做外自同构．因为 $b^{-1}(a^{-1}xa)b = (ab)^{-1}x(ab)$，而且 $a(a^{-1}xa)a^{-1} = x$，我们有

$$A_aA_b = A_{ab};\ A_{a^{-1}} = A_a^{-1}. \tag{6.2.3}$$

定理 6.2.1. 群 G 的内自同构组成 G 的全部自同构的群 $A(G)$ 的正规子群 $I(G)$．映射 $a\to A_a$ 是从 G 到 $I(G)$ 上的同态，它的核是 G 的中心．

证明. 根据 (6.2.3)，内自同构组成 $A(G)$ 的子群 $I(G)$．设 α 是 G 的任意自同构．那么 $(a^{-1}xa)^\alpha = (a^\alpha)^{-1}x^\alpha a^\alpha$． 于是 $\alpha^{-1}A_a\alpha$ 把 x 映成 $(a^\alpha)^{-1}xa^\alpha$，因而 $\alpha^{-1}(A_a)\alpha = A_{a^\alpha}$，所以 $I(G)$ 是 $A(G)$ 的正规子群. 根据 (6. 2. 3)，映射 $a\to A_a$ 是从 G 到 $I(G)$ 上的同态．现在 $A_a=1$ 必要而且只要对于每个 $x\in G$ 都有 $xa=ax$．因而 $A_a=1$ 必要而且只要 a 属于 G 的中心．因此同态 $G\to I(G)$ 的核是 G 的中心．

有限阿贝尔群 X 是它的西罗子群的直积 (定理 3. 2. 3)：

$$X = S(p_1)\times S(p_2)\times\cdots\times S(p_r). \tag{6.2.4}$$

X 的自同构群 $A(X)$ 必须包含自同构群 $A[S(p_i)]$ 的直积．但是因为 X 的自同构必须把每个 $S(p_i)(i=1,\cdots,r)$ 映到自身上，因此就不能再有其他的自同构，所以

$$A(X) = A[S(p_1)] \times \cdots \times A[S(p_r)]. \qquad (6.2.5)$$

更一般地，周期阿贝尔群的自同构群是其西罗子群的自同构群的笛卡儿乘积.

于是寻求周期阿贝尔群的自同构的问题简化成寻求阿贝尔 p 群的自同构. 有限阿贝尔 p 群 A_p 的任何自同构把一个基底映成另一个基底. 反之，设 $a_1, \cdots, a_s$ 和 $b_1, \cdots, b_s$ 是 A_p 的两个基底，它们按照定理 3.3.2 那样地编号，因而 a_i 与 b_i 的阶相同，$i = 1, \cdots, s$. 因为

$$\begin{aligned} A_p &= \{a_1\} \times \{a_2\} \times \cdots \times \{a_s\} \\ &= \{b_1\} \times \{b_2\} \times \cdots \times \{b_s\}, \end{aligned} \qquad (6.2.6)$$

所以映射

$$a_i \to (a_i)\alpha = b_i, \quad i = 1, \cdots, s \qquad (6.2.7)$$

决定 A_p 的一个自同构 α.

在 p 阶循环群 $C=\{a\}$，$a^p=1$ 内，每个元素 $a^i(i=1,\cdots,p-1)$ 都是生成元素. 因此由 $a \to (a)\alpha_i = a^i$ 决定的自同构有 $p-1$ 个. 如果 r 是模 p 的一个原根[1]，则 $a \to (a)\beta = a^r$ 决定一个自同构 β. 这时 $a \to (a)\beta^j = a^{r^j}$. 对于原根 r，使 $r^j \equiv 1 \pmod{p}$ 的 r 的第一个方次是 $j = p-1$. 因此自同构 β 的阶是 $p-1$，而且自同构群 $A(C)$ 是由 β 生成的 $p-1$ 阶循环群.

6.3. 群 的 全 形

G 的右和左正则表示都是 G 的元素的全体置换的群 S_G 的子群（§1.4). 其次，如果 α 是 G 的自同构，则 $\alpha: x \rightleftarrows x^\alpha$ 是

---

1) 关于原根的讨论参看 Birkhoff and Maclane[1] 第 446 页，或 Hardy and Wright[1] 第 236 页.（参看维诺格拉陀夫著《数论基础》，中译本，高等教育出版社，1956，第六章. ——译者）

S_G 中不变 G 的单位元素 1 的元素.

因为 $(g_1x)g_2=g_1(xg_2)$，我们有 $L(g_1)R(g_2)=R(g_2)\cdot L(g_1)$. 因此 G 的每个右正则表示和每个左正则表示都可交换.

定理 6.3.1. *G 的左右正则表示彼此是另一个在 S_G 内的中心化子.*

证明. 设 π 是 S_G 中属于 $L(G)$ 的中心化子的置换. 设 $(1)\pi=g$. 那么 $\pi R(g)^{-1}=\pi^*$属于 $L(G)$的中心化子而且不变单位元素$(1)\pi^*=1$. 这时$(1)\pi^*L(g')=g'$.因此还有 $(1)L(g')\pi^*=g'$，所以 $(g')\pi^*=g'$. 但是 g' 可以是 G 的任意元素，因而 $\pi^*=1$，所以 $\pi\in R(g)$. 因此 $L(G)$ 的中心化子是 $R(G)$. 同理 $L(G)$ 是 $R(G)$ 的中心化子.

这处理了 $R(G)$ 在 S_G 内的中心化子. 我们把 $R(G)$ 在 S_G 内的正规化子叫做 G 的*全形*.

定理 6.3.2. *设 H 是 G 的全形，即 $R(G)$ 在 S_G 内的正规化子. 那么 H 中不变 G 的 1 的子群是 G 的自同构群 $A(G)$.*

证明: 设 H 是 $R(G)$ 的正规化子而且 α 是 H 中不变 1 的一个元素. 这时 $R(g)\rightleftarrows\alpha^{-1}R(g)\alpha$ 当然是 $R(G)$ 的一个自同构，因为 $R(G)$ 是 H 的正规子群. 因此 $\alpha^{-1}R(g)\alpha=R(g^\alpha)$ 决定 G 到自身上的一个 1—1 映射 $g\rightleftarrows g^\alpha$. 但是因为在这个映射下 $(g_1g_2)^\alpha=g_1^\alpha g_2^\alpha$，所以 $g\rightleftarrows g^\alpha$ 是 G 的自同构，但是 α 实际上是置换 $g\rightleftarrows g^\alpha$. 因为 $(1)\alpha=1$ 和 $\alpha^{-1}R(g)\alpha=R(g^\alpha)$，我们有 $(1)\alpha R(g^\alpha)=g^\alpha$ 以及$(1)R(g)\alpha=g^\alpha$，因而 $(g)\alpha=g^\alpha$. 因此，如果 α 属于 H 而且不变 1. 则 α 是 G 的一个自同构. 反之，设 $\alpha:g\leftrightarrows g^\alpha$ 是 G 的一个自同构，那么 α 是 S_G 的不变 G 中的单位元素 1 的一个元素. 我们现在可以证明 $\alpha^{-1}R(g)\alpha=R(g^\alpha)$，因而 α 属于 $R(G)$ 的正规化子. 这是因为 $(x)R(g)\alpha=x^\alpha g^\alpha$，还有 $(x)\alpha R(g)=x^\alpha g^\alpha$. 因此 H 中不

变 1 的子群不仅由自同构组成，而且包含了每一个自同构. 在定理 6.3.1 的证明中，我们证明过只有 S_G 的单位元素不变 G 的 1 而且与 $R(G)$ 的每个元素都可交换. 因此 G 的每个自同构在 H 的不变 1 的子群中恰好出现一次，即这个子群是 $A(G)$. 因为群的正规化子包含它的中心化子，所以 $H \supset L(G)$.

6.4. 完 备 群

定义. 完备群是指中心是单位元素群而且全部自同构都是内自同构的群.

定理 6.4.1. 设 G 是完备群，它是群 T 的正规子群，那么 T 是 G 和 G 在 T 内的中心化子 K 的直积 $G \times K$.

证明. 设

$$T = G + Gx_2 + \cdots + Gx_i + \cdots. \tag{6.4.1}$$

这里 $x_i^{-1}Gx_i = G$，因为 G 在 T 内是正规的. 因而 $g \rightleftarrows x_i^{-1}gx_i = g^\alpha$ 是 G 的自同构. 因为 G 的每个自同构都是内自同构，对于某个 $a \in G$ 和所有的 g 有 $g^\alpha = a^{-1}ga$. 因此对于所有的 g 有 $x_i^{-1}gx_i = a^{-1}ga$. 这时 $y_i = x_ia^{-1}$ 属于 G 在 T 内的中心化子 K. 但是 $Gx_i = x_iG = x_ia^{-1}G = y_iG = Gy_i$，而且我们可以取 y_i 作为 G 的傍系代表. 因而 G 在 T 内的每个傍系包含 K 的一个元素. 于是由于 G 是正规的，$T = G \cup K = GK = KG$. 但是 $K \cap G = 1$，因为 G 的中心是单位元素群. 因此 $T = G \times K$，因为 K 的每个元素与 G 的每个元素可交换.

推论 6.4.1. 完备群 G 的全形 H 是直积 $R(G) \times L(G)$. 这是因为 $L(G)$ 是 $R(G)$ 在 H 内的中心化子.

6.5. 正规乘积(或半直积)

定理 6.5.1. 给了群 H 和 K，而且对于每个元素 $h \in H$ 给

了K的一个同构

$$k \rightleftarrows k^h \quad \text{对于所有 } k \in K, \tag{6.5.1}$$

使得

$$(k^{h_1})^{h_2} = k^{h_1 h_2}, \quad h_1, h_2 \in H. \tag{6.5.2}$$

于是符号 $[h, k]$, $h \in H$, $k \in K$ 在下列乘积规则下组成一个群:

$$[h_1, k_1] \cdot [h_2, k_2] = [h_1 h_2, k_1^{h_2} k_2], \tag{6.5.3}$$

它叫做K乘H的正规乘积或K乘H的半直积.

证明. 因为对于每个 k 和 h, $k^h \in K$, 乘积规则 (6.5.3) 是有定义的.

1) 乘积规则 (6.5.3) 是可结合的,因为利用 (6.5.1) 和 (6.5.2),

$$\begin{aligned}([h_1, k_1] \cdot [h_2, k_2]) \cdot [h_3, k_3] &= [h_1 h_2, k_1^{h_2} k_2] \cdot [h_3, k_3] \\ &= [(h_1 h_2) h_3, (k_1^{h_2} k_2)^{h_3} k_3] = [h_1 h_2 h_3, k_1^{h_2 h_3} k_2^{h_3} k_3], \end{aligned} \tag{6.5.4}$$

$$\begin{aligned}[h_1, k_1]([h_2, k_2] \cdot [h_3, k_3]) &= [h_1, k_1] \cdot [h_2 h_3, k_2^{h_3} k_3] \\ &= [h_1 h_2 h_3, k_1^{h_2 h_3} k_2^{h_3} k_3]. \end{aligned} \tag{6.5.5}$$

2) 元素 $[1,1]$ 是单位元素, 因为

$$[1, 1][h, k] = [1h, 1^h k] = [h, k],$$

$$[h, k][1, 1] = [h1, k^1 1] = [h, k].$$

这里 $k^1 = k$ 是根据 (6.5.2).

3) 任何 $[h, k]$ 都有一个左逆 $[h^{-1}, (k^{-1})^{h^{-1}}]$ (6.5.6)

$$[h^{-1}, (k^{-1})^{h^{-1}}] \cdot [h, k] = [h^{-1}h, k^{-1}k] = [1, 1].$$

因此具有乘积规则 (6.5.3) 的符号 $[h, k]$ 组成一个群 G.

定理 6.5.2. 如果G是K乘H的正规乘积, 则G的元素 $[h, 1]$ 组成一个子群同构于 H, 而且元素 $[1, k]$ 组成一个正规子群同构于 K. 其次,作为G的子群的K的自同构(6.5.1)由作为G的子群的H的元素 $h = [h, 1]$ 产生的变形所导出, 这是因为

$$[h,1]^{-1}[1,k][h,1]=[1,k^h]. \qquad (6.5.7)$$

再有，$G=H\cup K$，这是因为

$$[h,1][1,k]=[h,k]. \qquad (6.5.8)$$

证明. 我们只要注意到 $h \rightleftarrows [h,1]$ 和 $k \rightleftarrows [1,k]$ 是在 H 和 K 和 G 的子群之间的同构，这时用到规则 (6.5.3) 和 $k^1=k$. 再有，(6.5.7) 和 (6.5.8) 直接从规则 (6.5.3) 得出. 这时 (6.5.7) 指出 K 是正规子群而且自同构 (6.5.1) 是由元素 $h=[h,1]$ 产生的变形所导出的. 这时 $H\cap K=[1,1]=1$，而且 (6.5.8) 指出 H 的元素可以取作 K 的傍系代表.

定理 6.5.3. G 是 K 乘 H 的正规乘积，必要而且只要 K 是 G 的正规子群而且 H 是 G 的这样的子群，它的元素可以取作 K 的傍系代表. 换句话说，

1) K 是 G 的正规子群.

2) H 是 G 的子群.

3) $K\cap H=1$.

4) $H\cup K=G$.

证明. 我们已经看到当 G 是 K 乘 H 的正规乘积时，这些性质成立. 反之，假定这些性质成立. 那么由于 $K\cap H=1$，$H\cup K=G$ 而且 K 在 G 内是正规的，所以（定理 2.3.3）G 的每个元素可以唯一地表成

$$g=hk. \qquad (6.5.9)$$

因为 K 是正规的，

$$h^{-1}kh=k^h\in K, \qquad (6.5.10)$$

而且 $k \rightleftarrows k^h$ 显然是 K 的自同构. 其次，从 (6.5.10) 得出

$$(k^{h_1})^{h_2}=k^{h_1h_2}. \qquad (6.5.11)$$

对于 G 的两个元素的乘积表示，

$$g_1=h_1k_1,\quad g_2=h_2k_2,$$

$$g_1g_2=h_1k_1h_2k_2=h_1h_2(h_2^{-1}k_1h_2)k_2=h_1h_2\cdot k_1^{h_2}k_2, \qquad (6.5.12)$$

因而在G内的乘法规则正好与(6.5.3)相同,所以G是K乘H的正规乘积.

我们看到把K的一个自同构与H的一个元素结合是从H到K的自同构群的同态. 如果H被映成K的恒同自同构,即$k^h=k$对于每一个h和k,则(6.5.3)是H和K的直积的规则.

习　　题

1. 证明8阶的二面体群同构于它的自同构群.
2. 证明p^r阶的初等阿贝尔群的自同构群的阶是$(p^r-1)(p^r-p)\cdots(p^r-p^{r-1})$.
3. 求六个文字上的对称群S_6的一个外自同构. 这个自同构交换两组3阶元素.
4. 证明,如果群G的阶能被p^2(素数的平方)整除,则它的自同构群的阶能被p整除.(提示:如果不存在p阶的内自同构,则可以证明有一个西罗p子群是阿贝尔群而且是G的直接因子.)
5. 群G的自同构α叫做中心自同构,假如对于每个$x\in G$,$x^{-1}(x)\alpha\varepsilon Z$,这里$Z$是$G$的中心. 证明中心自同构(它们都是$G$的内自同构)的群同构于$G/Z$的中心.
6. 设G是由元素a, b, c生成的群,满足定义关系$a^8=b^8=c^4=1, b^{-1}ab=a^5, c^{-1}ac=a^3, c^{-1}bc=a^6b$. 证明$\{a, b\}$是$\{a\}$乘$\{b\}$的正规乘积,而且$G$是$\{a,b\}$乘$\{c\}$的正规乘积. 由此得出结论:这些关系定义一个256阶群,它的元素有形状$a^ib^jc^k$.
7. 设G是习题6中的群. 证明$\alpha: a\to a^5,\ b\to b,\ c\to c$是$G$的外自同构,它把$G$的每个共轭类都变到自身.

第七章　自　由　群

7.1.　自由群的定义

设给了一组元素 $S=s_1,\cdots,s_n$，这时并不假定元素 $s_1,\cdots,s_n$ 的个数是有限的或可数的．但是在需要的时候，我们将假定 s_i 的指标 i 是良序的．我们再定义符号 s_i^1，s_i^{-1}，这里 $s_i^1=s_i$ 而 s_i^{-1} 是新的符号．

字或串是指空集（写成 1）或有限序列 $a_1a_2\cdots a_i$，这里每个 a_i 是 s_j^ε，$\varepsilon=\pm1$ 中的一个．

字叫做简化字，假如它是空集或者在 $a_1\cdots a_t$ 中没有对于 a_ia_{i+1} $(i=1,\cdots,t-1)$ 是 $s_j^\varepsilon s_j^{-\varepsilon}$ $(\varepsilon=\pm1)$ 的形式．

如果字 $f_1=gs_j^\varepsilon s_j^{-\varepsilon}h$ 和 $f_2=gh$，则这两个字 f_1 和 f_2 叫做邻接的．

给了字 f 和 g，如果存在 $f_1=f$，f_2，$\cdots$，$f_m=g$，使得 f_i 和 f_{i+1} 对于 $i=1,\cdots,m-1$ 都是邻接的，则 f 和 g 叫做等价的，而且记做 $f\sim g$．$f\sim g$ 显然是真的等价关系．等价于 f 的全体字组成一类，我们记做 $[f]$．

引理 7.1.1.　每一类包含一个而且仅包含一个简化字．

证明．如果 $f=a_1\cdots a_t$ 包含任何 $a_ia_{i+1}=s_j^\varepsilon s_j^{-\varepsilon}$，则就有邻接于 f 的字 $a_1\cdots a_{i-1}a_{i+1}\cdots a_t$ 包含较少的符号．经过最多 $t/2$ 步逐次化简，我们就能得出等价于 f 的简化字．这说明 $[f]$ 至少包含一个简化字．

现在对于 $f=a_1a_2\cdots a_t$ 我们定义 W 过程：

$W_0=1$　　　　空字

$$W_1 = a_1$$

$$W_{i+1} = W_i a_{i+1} \qquad \text{如果 } W_i \text{ 不是简化形式 } Xa_{i+1}^{-1}$$

$$= X \qquad \text{如果 } W_i \text{ 是简化形式 } Xa_{i+1}^{-1}.$$

根据归纳法可以得出，$W_0, W_1, \cdots, W_t$ 都是简化的形式，而且当 f 是简化形式时，$W_t = f$. 现在设

$$f_1 = a_1 \cdots a_r a_{r+1} \cdots a_t,$$

$$f_2 = a_1 \cdots a_r s_j^{\epsilon} s_j^{-\epsilon} a_{r+1} \cdots a_t,$$

我们用 $W_0^1, W_1^1, \cdots, W_t^1$ 表示 f_1 的 W 过程中的字，而且用 $W_0^2, W_1^2, \cdots, W_{t+2}^2$ 表示 f_2 的 W 过程中的字. 我们希望证明 $W_t^1 = W_{t+2}^2$. 这时 $W_0^1 = W_0^2, \cdots, W_r^1 = W_r^2$，因为这些过程是相同的. 考虑两种情形：

1) $W_r^1 = W_r^2$ 是简化的形式 $Xs_j^{-\epsilon}$. 因为 $Xs_j^{-\epsilon}$ 是简化形式，所以 X 不是简化形式 Ys_j^{ϵ}. 于是对于 f_2，$W_{r+1}^2 = X$，$W_{r+2}^2 = Xs_j^{-\epsilon} = W_r^2 = W_r^1$.

2) $W_r^1 = W_r^2$ 不是简化的形式 $Xs_j^{-\epsilon}$. 这时 $W_{r+1}^2 = W_r^2 s_j^{\epsilon}$，$W_{r+2}^2 = W_r^2 = W_r^1$.

因此在这两种情形里都有 $W_{r+2}^2 = W_r^1$，所以可以归纳地得出 $W_{r+2+i}^2 = W_{r+i}^1$，因为这些过程是相同的. 于是 W 过程对于任何两个邻接的字（因而也对于任何两个等价的字）产生相同的简化字. 但是 W 过程不会变动简化字. 因此不会在同一个类里存在两个不同的简化字.

我们可以为这些字类定义一种乘法，而且在这个定义下这些类组成一个群，它就叫做由 S 生成的自由群 F.

定理 7.1.1. 对于 S 上的任何两个字类 $[f_1]$ 和 $[f_2]$，定义它们的乘积 $[f_1][f_2] = [f_1f_2]$. 这个乘积是有意义的，而且 S 上的全体字类对于这个乘积而说组成一个群，叫做由 S 生成的自由群 F.

证明. 假定 $f_1 \sim f_1'$，$f_2 \sim f_2'$. 那么 $f_1f_2 \sim f_1'f_2'$，因为我们

可以依次通过邻接的字把 f_1 换成 f_1'，先证明 $f_1f_2 \sim f_1'f_2$. 同理 $f_1'f_2 \sim f_1'f_2'$，因而 $f_1f_2 \sim f_1'f_2'$，因而 $[f_1'f_2'] = [f_1f_2]$，所以乘积 $[f_1f_2] = [f_1][f_2]$ 只取决于 f_1 和 f_2 的类而不取决于特别的代表. 空字是这个乘积的单位元素，因为 $[1][f]=[f][1]=[f]$. 其次，如果 $f = a_1\cdots a_t$ 而且 $h = a_t^{-1}\cdots a_1^{-1}$，则 $[f][h] = [fh] = [1]$ 和 $[h][f] = [hf] = [1]$. 因此 $[a_t^{-1}\cdots a_1^{-1}]$ 是类 $[a_1\cdots a_t]$ 的逆. 再有我们发现 $([f_1][f_2])[f_3] = [f_1f_2f_3] = [f_1]([f_2][f_3])$，因而结合律成立. 因此字类组成一个群，它叫做由 S 生成的自由群 F. 为了指明生成集合也记做 F_S.

当两个字等价因而代表 F 的同一个元素时，写成 $f_1 = f_2$ 是合适的. 我们还用 $f_1 \equiv f_2$ 表示 f_1 和 f_2 是同一个字. 用字的简化形式来代表 F 的元素自然是比较合适的. 因此当 $f= a_1\cdots a_t$ 是简化形式时，我们说 f 是写成简化形式的.

在任何群 G 内，一组元素 $X: x_1, \cdots, x_n$ 生成一个子群 H，它由全体有限乘积 $b_1, b_2\cdots b_t$ 组成，这里每个 b_j 是某个 x_j^ϵ，$\epsilon = \pm 1$. 要验证这些有限乘积组成子群是不困难的. 一般地说，H 的元素可以用很多方式写成这样的有限乘积. 其次，G 的全体元素显然生成 G. 因此每个群 G 都可以认为是由一组元素 X 生成的，我们记做 $G = \{X\}$. 下列定理说明为什么自由群不仅本身值得注意，而且是研究所有的群的工具.

定理 7.1.2. 设群 G 由一组元素 X: $x_1, \cdots, x_n$ 生成. 那么如果 F 是由 S:$s_1, \cdots, s_n$ 生成的自由群，则就存在由 $s_i \to x_i$（对于所有 i）决定的同态 $F \to G$.

证明. 设 $f = a_1\cdots a_t$ 是 S 的任意字. 考虑元素 $g= b_1\cdots b_t \in G$，这里当 $a_i = s_j^\epsilon$ 时取 $b_i = x_j^\epsilon$. 那么 $f \to g$ 把 S 的每个字映成 G 的一个元素. S 的邻接的(因而还有等价的)字显然映成 G 的同一个元素. 因此映射 $f \to g$ 确实是把 F 的元素映成 G 的元素的映射. 其次，如果 $f_1 \to g_1$，$f_2 \to g_2$，则 $f_1f_2 \to$

g_1g_2. 因此映射 $s_i \to x_i$ 决定从 F 到 G 上的一个同态. 根据同态定理，我们有下列推论:

推论 7.1.1. 作为由集合 X 生成的群而给出的任何群 G，是具有同样个数生成元素的自由群 F 的商群.

下面是自由群的另一个定义:

定义. 由一组元素 S 生成的自由群 F 是具有下列性质的群:

1) F 由 S 生成.

2) 如果 G 是由一组元素 X 生成的任意群，而且在 S 和 X 之间存在一一对应 $S \rightleftarrows X$，则就存在从 F 到 G 上的同态 $F \to G$ 把 S 映成 X.

利用定理 7.1.2 可以证明这是恰当的定义. 根据前一个定义，自由群 F_S 满足这些要求. 其次，如果 F' 是由 S 生成的群而且 $F' \to F_S$，则因为只有 F' 的单位元素才能映成单位元素，所以这个同态必定是同构.

然而在这个定义中有些不妥之处. 它不是一个构造性定义，而且没有前面的构造过程，无法说明具有性质 1 和 2 的群存在，也无法说明即使这样的群存在，也并没有非显然的关系成立. 其次，从较广的角度看来，“自由”体系是在其中除从公理推得的关系外没有其他关系成立的体系，这种体系的概念即使在类似于定理 7.1.2 的定理不成立时，也是值得探讨的.

7.2. 自由群的子群.施赖尔方法

子群的本质在研究群时常常是基本的，而对于自由群说，根据定理 7.1.2，正规子群是特别值得注意的. 臬尔逊 (Nielson[1]) 和施赖尔 (Schreier[3]) 证明过，自由群的子群本身是

自由群．臬尔逊的证明只对有限生成群成立，但是他的证明曾被勒维（Levi[1]）和别人推广而解除了这个限制．臬尔逊的方法直接处理子群的元素，施赖尔的方法则处理子群的傍系．这里给出的第一个证明[1]是施赖尔方法的一种简化．

自由群 F 的一组元素 G 叫做施赖尔组，假如对于每个 $g\in G$：

1） $g=a_1a_2\cdots a_t$ 是写成简化形式的．

2） $a_1a_2\cdots a_{t-1}$ 也是 G 的元素．

我们说 G 是双侧施赖尔组，假如除 1 和 2 外，还有下列条件成立：

3） $a_2\cdots a_t$ 也是 G 的元素．

注意施赖尔组总包含单位元素．

设 F 是由 S 生成的自由群而且 U 是 F 的子群．考虑 F 对 U 的左傍系分解：

$$F=U\cdot 1+Ug_2+\cdots+Ug_i+\cdots. \qquad (7.2.1)$$

我们总取单位元素作为 U 本身的代表元素．我们发觉最好取其余傍系的代表使得它们满足某些关系．

引理 7.2.1（推广的施赖尔引理）．如果 U 是自由群 F 的子群，则可以选取 U 的左傍系的代表来组成一个施赖尔组．如果 U 是 F 的正规子群，则可以选取傍系的代表来组成一个双侧施赖尔组．

证明．设 F 的生成元素 S：$s_1,\cdots,s_n$ 和它们的逆以任何方式排成良序；例如当 n 是有限数时排成 $s_1<s_1^{-1}<s_2<s_2^{-1}<\cdots<s_n<s_n^{-1}$．但是并未假定集合 S 是有限的或可数的，而只不过假定集合 $S\cup S^{-1}$ 是良序的．

$S\cup S^{-1}$ 的这个顺序可以扩大成 F 的全体元素的一个字典

1）参看 M. Hall and Rado[1]，进一步的结果参看 M. Hall[4,5]．

顺序．如果有 F 的两个元素 f 和 g，则我们可按字典顺序来定义 $f < g$，假如 f 和 g 的简化形式是

$$f = a_1 \cdots a_t,$$
$$g = b_1 \cdots b_u,$$

这里 a_i 和 b_j 属于 $S \cup S^{-1}$，而且下列条件有一个成立：

1) $t < u$.

2) $t = u$, $a_1 < b_1$.

3) $t = u$; $a_1 = b_1, \cdots, a_i = b_i; a_{i+1} < b_{i+1}$.

这样定义的字典顺序显然是一个全序，甚至还是良序，而且下列有用的性质成立：

如果 $f < g$ 而且 gh 写成简化形式，则 $fh < gh$. 如果 $f < g$ 而且 hg 写成简化形式，则 $hf < hg$. 这可以用顺序的定义来验证.

为了证明引理，我们取傍系 Ug_i 的代表元素 g_i 为傍系中在 F 的字典顺序里最前的元素． 然后我们来证明 g_i 组成施赖尔组，而且当 U 是正规子群时还是双侧施赖尔组．因为单位元素是 F 的第一个元素，单位元素就选作子群 U 的代表元素．设 $g = a_1 \cdots a_{t-1} a_t$ 是傍系 Ug 的代表，它是这个傍系内的最前的元素． 设 h 是在包含 $h^* = a_1 \cdots a_{t-1}$ 的傍系内的最前的元素． 如果 $h = b_1 \cdots b_u$，则 $h \leqslant a_1 \cdots a_{t-1}$. 但是 $ha_t \in Ug$，因而 $g \leqslant ha_t$. 再有 $ha_t \leqslant a_1 \cdots a_{t-1} a_t = g$. 因此 $g = ha_t$，即 $h = h^* = a_1 \cdots a_{t-1}$ 也是傍系代表． 于是这些 g 组成施赖尔组．如果 U 是正规子群，设 $a_2 \cdots a_t$ 在傍系 $Uf = fU$ 内，它的最前的元素是 f. 那么 $f \leqslant a_2 \cdots a_t$ 而且 $a_1 f$ 属于傍系 $a_1 \cdots a_t U = gU = Ug$. 于是 $g \leqslant a_1 f$. 但是还有 $a_1 f \leqslant a_1 a_2 \cdots a_t = g$. 因而 $g = a_1 f$ 而且 $f = a_2 \cdots a_t$. 因此这些 g 组成双侧施赖尔组．注意引理只不过保证由左傍系代表组成的施赖尔组的存在．同一个子群可以具有多于一个的傍系代表组是

施赖尔组.

主要定理: 定理 7.2.1. 自由群的子群是自由群.

设 F 是由集合 S 生成的自由群而且 U 是 F 的已知子群. 那么根据施赖尔引理, 我们可以假定左傍系代表组 G 是施赖尔组.

$$F = U \cdot 1 + Ug_2 + \cdots + Ug_i + \cdots. \qquad (7.2.2)$$

我们先证明一个引理, 它对于任何群 F (不管是否自由群) 都成立. 设 F 由一组元素 S 生成, U 是 F 的子群而且 (7.2.2) 是 F 对 U 的左傍系分解.

如果 F 的元素 f 属于 (7.2.2) 中的傍系 Ug_i, 我们用 $\Phi(f) = g_i$ 来定义一个函数 $\Phi(f)$. 于是对于 $u \in U$, $\Phi(uf) = \Phi(f)$. $\Phi(f) = 1$ 必要而且只要 $f \in U$.

假定 $f = a_1a_2\cdots a_t$, 这里每个 $a_i \in S \cup S^{-1}$. 记 $f_0 = 1$, $f_1 = a_1$, $f_2 = a_1a_2$, $\cdots$, $f_t = a_1a_2\cdots a_t = f$. 然后记 $h_0 = \Phi(f_0) = 1$, $h_1 = \Phi(f_1)$, $\cdots$, $h_t = \Phi(f)$. 那么当 $f \in U$ 因而 $h_t = 1$ 时, 我们有

$$fh_t^{-1} = h_0a_1h_1^{-1} \cdot h_1a_2h_2^{-1} \cdot h_2 \cdots h_{t-1}^{-1} \cdot h_{t-1}a_th_t^{-1} = f. \qquad (7.2.3)$$

现在因为 $h_i = \Phi(h_i) = \Phi(f_i) = \Phi(f_{i-1}a_i) = \Phi(h_{i-1}a_i) = \Phi(h_{i-1}s_\alpha^\epsilon)$, $a_i = s_\alpha$, $\epsilon = \pm 1$, $h_i \in G$, 显然在 (7.2.3) 内只需要这样的函数 Φ, 它的元有形状 $gs^\epsilon (g \in G,\ s^\epsilon \in S \cup S^{-1})$. 然后我们记 $\phi(gs^\epsilon) = \Phi(gs^\epsilon)$, 使得 $\phi(f)$ 只对元 $f = gs^\epsilon$ 有定义.

引理 7.2.2. 在任何群 F 内, 元素 $gs\phi(gs)^{-1}$ 是子群 U 的生成元素, 这里 g 遍历 U 在 (7.2.2) 里的左傍系代表, s 遍历 F 的生成元素, 而且 $\phi(gs^\epsilon)$ 是包含 gs^ϵ 的傍系的代表.

证明. 如果 $f \in U$, 则 $h_t = 1$ 而且 (7.2.3) 表明 f 是元素 $h_{i-1}a_ih_i^{-1}$ 的乘积, 而且因为 $h_i = \Phi(h_{i-1}a_i)$, 所以 $h_{i-1}a_ih_i^{-1}$ 有形状 $gs^\epsilon\phi(gs^\epsilon)^{-1}$, 这里 $h_{i-1} = g$ 和 $a_i = s^\epsilon$, 因而 $h_i = \phi(gs^\epsilon)$.

但是 $gs^\epsilon\in U\phi(gs^\epsilon)$，因而对于任何 gs^ϵ，元素 $gs^\epsilon\phi(gs^\epsilon)^{-1}\in U$. 意如果 $\phi(g_js^\epsilon)=g_k$，则 $\phi(g_ks^{-\epsilon})=g_j$. 因此如果 $g_js^\epsilon\phi(g_js^\epsilon)^{-1}=g_js^\epsilon g_k^{-1}$,则它的逆是 $g_ks^{-\epsilon}g_j^{-1}=g_ks^{-\epsilon}\phi(g_ks^{-\epsilon})^{-1}$，它具有同样的形状，只是在 s 的方幂上有相反的符号. 因此元素 $gs\phi(gs)^{-1}$ 生成 U.

推论 7.2.1. 如果 F 是有限生成群而且 U 是在 F 内具有有限指数的子群，则 U 是有限生成的.

这是因为对于 $gs\phi(gs)^{-1}$ 中的 g 和 s，只存在有限种选择.

从现在起,我们假定 F 是自由群,而且傍系代表组 G 是施赖尔组.

我们将利用函数 $\phi(gs^\epsilon)$ 的下列性质:

1) $\phi(gs^\epsilon)\in G$.

2) 如果 $gs^\epsilon\in G$，则 $\phi(gs^\epsilon)=gs^\epsilon$.

3) $\phi[\phi(gs^\epsilon)s^{-\epsilon}]=g$.

作为通用的记号，我们记 $v=gs^\epsilon\phi(gs^\epsilon)^{-1}$ 和 $u=gs\phi(gs)^{-1}$. 因而 u 是 s 的方次为 $+1$ 的 v，而 v 或是 u 或是 u 的逆，因为如果 $v=g_is^{-1}\phi(g_is^{-1})^{-1}$,则令 $\phi(g_is^{-1})=g_j$. 然后根据第三个性质，$v^{-1}=g_jsg_i^{-1}=g_js\phi(g_js)^{-1}$ 是 u，同理可证 u 的逆是 v.

引理 7.2.3. $v=gs^\epsilon\phi(gs^\epsilon)^{-1}$ 或是写成简化形式的,或是 1.

证明. 设 $v=g_js_a^\epsilon\phi(g_js_a^\epsilon)^{-1}=g_js_a^\epsilon g_k^{-1}$,这里 $g_k=\phi(g_js_a^\epsilon)$. g_j 和 g_k^{-1} 都是写成简化形式的. 因此,如果在 v 内可以作任何简化,则或者 (1) g_j 以 $s_a^{-\epsilon}$ 结尾，或者 (2) g_k^{-1} 以 $s_a^{-\epsilon}$ 开始. 如果 (1) 成立，则 $g_j=a_1\cdots a_{t-1}s_a^{-\epsilon}$ 是 g_j 的简化形式,因而 $g_js_a^\epsilon=a_1\cdots a_{t-1}$ 是一个 g，而且根据函数 ϕ 的性质 2，$g_k=\phi(g_js_a^\epsilon)=g_js_a^\epsilon$；所以 $v=g_js_a^\epsilon g_k^{-1}=1$. 如果 (2) 成立，则同理 $g_j=(g_ks_a^{-\epsilon})=g_ks_a^{-\epsilon}$，仍然有 $v=1$.

对于 $v=gs^\epsilon\phi(gs^\epsilon)^{-1}\neq 1$，我们把因子 s^ϵ 叫做 v 的有效

因子. 假定 $v = g_j s_a^\epsilon \phi(g_j s_a^\epsilon)^{-1} = g_k s_b \phi(g_k s_b)^{-1} \neq 1$. 如果 g_j 和 g_k 是同样长的,则因为 v 写成了简化形式, $g_j = g_k$, $s_a = s_b$. 如果 g_j 和 g_k 长度不同,例如 g_k 长些, 则 $g_j s_a^\epsilon$ 作为 g_k 的前面部分本身是一个 g; 所以 $\phi(g_j s_a^\epsilon) = g_j s_a^\epsilon$, 因而 $v = 1$ 而与假设矛盾. 因此 $v \neq 1$ 只能唯一地表成 $gs^\epsilon\phi(gs^\epsilon)^{-1}$, 特别也就只有唯一的有效因子.

引理 7.2.4. 在乘积 v_1v_2 内, 这里 $v_1 \neq 1$, $v_2 \neq 1$, $v_2 \neq v_1^{-1}$, 在消去时不可能达到每个 v 的有效因子.

证明. 设 $v_1 = g_i s_a^\epsilon g_j^{-1}$, $g_j = \phi(g_i s_a^\epsilon)$, $v_2 = g_k s_b^\eta g_l^{-1}$, $g_l = \phi(g_k s_b^\eta)$. v_1 和 v_2 都写成简化形式,而且因为 $v_2 \neq v_1^{-1}$, 我们不可能同时有 $g_k = g_j$ 和 $s_b^{-\eta} = s_a^\epsilon$. 让我们否定这个引理而假定消去时能达到一个有效因子. 如果消去先达到 s_b^η, 则 $g_k s_b^\eta$ 是 g_j 的前面部分,因而 $\phi(g_k s_b^\eta) = g_k s_b^\eta$ 而且 $v_2 = 1$, 与假设矛盾. 同理,如果消去先达到 s_a^ϵ, 则 $g_i s_a^{-\epsilon}$ 是 g_k 的前面部分因而 $v_1 = 1$, 也与假设矛盾. 又如果消去同时包括 s_a^ϵ 和 s_b^η, 则 $g_k = g_j$, $s_b^\eta = s_a^{-\epsilon}$, 因而 $v_2 = v_1^{-1}$, 也与假设矛盾.

现在我们已经接近主要定理的证明了.

引理 7.2.5. 几个 v 的乘积 $v_1v_2\cdots v_m$, $v_i \neq 1$, $i = 1, \cdots, m$, $v_{i+1} \neq v_i^{-1}$, $i = 1, \cdots, m-1$, 不可能是单位元素.

证明. 重复应用引理 7.2.4, 在 v_i 和 v_{i+1} 之间消去时不能达到每一个的有效因子. 因此在把它们写成以 s 表出的简化形式时, 乘积 $v_1\cdots v_m$ 包含全体原有的有效因子,因而不可能是单位元素.

现在我们来讨论元素 u, $u = gs\phi(gs)^{-1} \neq 1$. 根据引理 7.2.2. 全体 u 生成 U, 因而全体 $u \neq 1$ 生成 U. 如果作为以 u 表出的简化字的 u 的乘积没有等于 1 的, 即用 s 表出时没有简化成 1 的, 则这些 u 是 U 的自由生成元素. 但是每个 $v \neq 1$ 是 u 或 u^{-1}, 而且恰好只是一种方式. 因此以 $u \neq 1$ 表

出的简化字将有在引理 7.2.5 里处理过的形式 $v_1v_2\cdots v_m$，$v_i\neq 1$，$v_{i+1}\neq v_i^{-1}$，因而不会是单位元素．因此下面的引理 7.2.6 成立．

引理 7.2.6. 元素 $u=gs\phi(gs)^{-1}\neq 1$ 是 U 的自由生成元素．

于是我们找到了 U 的自由生成元素，因而 U 是自由群．

在引理 7.2.4 中的有效因子的地位是定理 7.2.1 的这个证明的关键．我们可以用有效因子的一个独立定义来推广这个观念．

元素集合 Y 满足 $Y\cap Y^{-1}=0$ 说是具有有效因子的，假如对于每个 $y\in Y$，我们可以从 y 和 y^{-1} 的简化形式选出一个因子：

$$y=a_1\cdots a_i\cdots a_t,$$
$$y^{-1}=a_t^{-1}\cdots a_i^{-1}\cdots a_1^{-1},$$

从 y 选出 a_i 和从 y^{-1} 选出 a_i^{-1} 要使得在任何乘积

$$zw, z\neq w^{-1},\quad z,w\in Y\cup Y^{-1}$$

内消去时不会达到 z 或 w 的有效因子．换句话说，Y 具有有效因子，假如在 $Y\cup Y^{-1}$ 内引理 7.2.4 对于这些因子成立．集合 Y 的有效因子叫做中心有效因子，假如对于一个奇数长度的 y，有效因子是它的中心项，而对于一个偶数长度的 y，有效因子是它的两个中心项中的一个．

定理 7.2.2. 如果集合 Y 具有有效因子，则 Y 的元素是由它们生成的子群的自由生成元素．如果 G 是施赖尔组，它的每个 g 都是傍系 Ug 的最短元素，则对于 $u=gs\phi(gs)^{-1}\neq 1$ 的那些 u，其中的 s 都是中心有效因子．

证明．根据有效因子的定义，引理 7.2.4 对于 $v_1,v_2\in Y\cup Y^{-1}$ 成立．于是引理 7.2.5 也成立．因此以这些 y 和它们的逆表出的字没有一个是单位元素，除非它以这些 y 表出的简

化形式是单位元素；因而这些 y 是由它们生成的群的自由生成元素.

如果 G 是由子群 U 的傍系代表 g 组成的施赖尔组，使得有一个傍系 Ug 不包含短于 g 的元素，则因为

$$gs \in U\phi(gs),$$
$$\phi(gs)s^{-1} \in Ug,$$

所以 g 和 $\phi(gs)$ 的长度最多相差一. 因此，在引理 7.2.4 中已经证明是有效因子的 s 是中心有效因子，因为在 $u = gs\phi(gs)^{-1}$ 中它处在长度最多相差一的两个字的中间.

我们可以来证明引理 7.2.6 和主要定理的一个逆命题.

定理 7.2.3. 设 G 是由自由生成组 S 生成的群 F 的施赖尔组. 设 $\phi(h)$ 是对于元 $h = gs^\epsilon, \epsilon = \pm 1, g \in G, s \in S$ 有定义的函数，满足

1）$\phi(gs^\epsilon) \in G$.

2）如果 $gs^\epsilon \in G$，则 $\phi(gs^\epsilon) = gs^\epsilon$.

3）$\phi[\phi(gs^\epsilon)s^{-\epsilon}] = g$.

那么元素 $u = gs\phi(gs)^{-1} \neq 1$ 是 F 的一个子群 U 的自由生成元素，而且施赖尔组 G 是 U 在 F 内的左傍系代表组.

证明. 我们记 $v = gs^\epsilon\phi(gs^\epsilon)^{-1}$ 作为一个通用的记号. 在这里所给的假设下，引理 7.2.3, 7.2.4 和 7.2.5 的证明都有效，因为在这些引理的证明中只用到函数 ϕ 的上述性质. 从引理 7.2.5 得出元素 $u = gs\phi(gs)^{-1} \neq 1$ 是 F 的某个子群 U 的自由生成元素.

为了证明施赖尔组 G 是 U 的左傍系代表组，我们对于 $S \cup S^{-1}$ 中的每个字 f 定义函数 $\Phi(f)$. 假定

$$f = a_1a_2\cdots a_t,\quad a_i \in S \cup S^{-1},\quad i = 1, \cdots, t.$$

令

$$h_0 = 1,$$

$$h_i = \phi(h_{i-1}a_i),\ i = 1,\cdots,t,$$
$$h_t = \Phi(f).$$

容易证明 $\Phi(f)$ 的主要性质是:

1) $\Phi(a_1\cdots a_i a_{i+1}\cdots a_t) = \Phi(a_1\cdots a_i s^\varepsilon s^{-\varepsilon} a_{i+1}\cdots a_t)$.

根据定义，每个 $h_i\ (i = 1,\cdots,t)$ 是一个 $g \in G$. 因此在计算右边的值时我们依次得到 $h_i, \phi(h_i s^\varepsilon)$ 和 $\phi[\phi(h_i s^\varepsilon)\cdot s^{-\varepsilon}] = h_i$ (根据性质 (3)). 否则计算两边的值的过程是全同的. 因而 $\Phi(f)$ 对于代表 F 的同一个元素的两个字是相同的.

2) $\Phi(g) = g$.

这时如果 $g = a_1,\cdots,a_t$ 是一个 $g \in G$ 的简化形式,则它的任何前面部分也是一个 g, 因而根据性质 (2), $h_i = a_1\cdots a_i$, $i = 1,\cdots,t$.

3) $\Phi(f_1 f_2) = \Phi[\Phi(f_1) f_2]$.

记 $f = f_1 f_2$, $f_1 = a_1\cdots a_i$, $f_2 = a_{i+1}\cdots a_t$. 那么 $h_i = \Phi(f_1)$ 是一个 g, 因而 $\Phi(h_i) = h_i$. 因此在计算 $\Phi(h_i f_2)$ 的值时，我们有一项等于 h_i, 于是以后的项等于 $h_{i+1}\cdots h_t = \Phi(f_1 f_2)$.

4) $\Phi(gs^\varepsilon) = \phi(gs^\varepsilon)$.

这时根据函数 Φ 的定义, $\Phi(gs^\varepsilon) = \phi(\Phi(g)s^\varepsilon)$. 因为 $\Phi(g) = g$, 所以 $\Phi(gs^\varepsilon) = \phi(gs^\varepsilon)$.

5) $\Phi[gs^\varepsilon \phi(gs^\varepsilon)^{-1}] = 1$.

这时 $\Phi[gs^\varepsilon\phi(gs^\varepsilon)^{-1}] = \Phi[\Phi(gs^\varepsilon)\phi(gs^\varepsilon)^{-1}] = \Phi[\phi(gs^\varepsilon)\cdot\phi(gs^\varepsilon)^{-1}] = \Phi(1) = 1$.

6) 如果 $f \in U$, 则 $\Phi(f) = 1$.

重复应用 (3) 和 (5) 就能得出这个结果.

7) 如果 $\Phi(f) = g$, 则 $f \in Ug$.

这时 $f = a_1 a_2\cdots a_t$

$$= (1\cdot a_1\cdot h_1^{-1})(h_1 a_2 h_2^{-1})\cdots(h_{t-1}a_t h_t^{-1})h_t,$$

而且每个 $h_{i-1}a_i h_i^{-1} = gs^\varepsilon\phi(gs^\varepsilon)^{-1} \in U$, $i=1,\cdots,t$, 再有 $h_t=$

$\Phi(f)=g$. 特别地，如果 $\Phi(f)=1$，则 $f\in U$.

8）如果 $g_i\neq g_j$，则 g_i 和 g_j 在 U 的不同傍系内.

否则 $g_i=wg_j$,这里 $w\in U$，因而 $g_i=\Phi(g_i)=\Phi[\Phi(w)\cdot g_j]=\Phi(g_j)=g_j$，这是一个矛盾.

总之我们证明了傍系 Ug 全不相同而且穷尽了整个自由群 F. 在证明定理 7.2.3 时，我们所证明的已超过了原来所要求的. 我们把这也写成一个定理.

定理 7.2.4. 给了施赖尔组 G 和定理 7.2.3 的函数 $\phi(gs^\varepsilon)$. 单从这些就能判定任意元素 f 是否属于由 G 和 ϕ 决定的子群 U.

证明. 我们可以从 ϕ 和 G 来计算 $\Phi(f)$，并且 $\Phi(f)=1$ 必要而且只要 $f\in U$. 因为 ϕ 和 G 以显明的方式决定 U,我们可以认为 ϕ 和 G 表示了 U，而且说 $U=U[G,\ \phi(gs^\varepsilon)]$ 是 U 的标准表示.

自然会产生两个问题：

1）同一个子群的两个不同的标准表示彼此有何关系?

2）一个给定的施赖尔组能表示多少个子群（如果有的话)?

我们将要依次来回答这两个问题.

定理 7.2.5. $U_1=U_1[G_1,\ \phi_1(gs^\varepsilon)]$ 和 $U_2=U_2[G_2,\phi_2(gs^\varepsilon)]$ 是同一个子群，必要而且只要在施赖尔组 G_1 和 G_2 之间有一个一一对应 $g^1\rightleftarrows g^2$，包括 $1\rightleftarrows 1$，使得从 $g^1\rightleftarrows g^2$ 得出 $\phi_1(g^1s^\varepsilon)\rightleftarrows\phi_2(g^2s^\varepsilon)$ 对于任何 s^ε.

证明. 如果 $U_1=U_2=U$，则 U 的每个傍系在 G_1 和 G_2 内各有一个代表. 因而如果 $Ug^1=Ug^2$，则对应 $g^1\rightleftarrows g^2$ 显然是一一的而且包括 $1\rightleftarrows 1$. 因为 g^1s^ε 和 g^2s^ε 在同一个傍系内，所以 $\phi_1(g^1s^\varepsilon)=\phi_2(g^2s^\varepsilon)$.

反之，假定给了包括 $1\rightleftarrows 1$ 的一一对应 $g^1\rightleftarrows g^2$，使得

在所有情形里都有 $\phi_1(g^1s^\varepsilon)\rightleftarrows\phi_2(g^2s^\varepsilon)$. 我们发现对于每个 f 都有 $\Phi_1(f)\rightleftarrows\Phi_2(f)$，特别地，$\Phi_1(f)=1$ 必要而且只要 $\Phi_2(f)=1$. 这是说 U_1 和 U_2 包含同一个元素 f，因而是同一个子群 U. 其次，对 g^1 的长度施行归纳法可以证明 $Ug^1=Ug^2$.

在回答第二个问题之前我们先提出函数 ϕ 的几个性质. 对于全体 $g\in G$ 和固定的生成元素 s 的映射 $\pi(s):g\to\phi(gs)$ 和 $\pi(s^{-1}):g\to\phi(gs^{-1})$ 都把整个 G 映到自身. 根据映射 ϕ 的性质 (3)，乘积 $\pi(s)\pi(s^{-1})$ 和 $\pi(s^{-1})\pi(s)$ 都是单位元素. 因此 $\pi(s)$ 和 $\pi(s^{-1})$ 都是置换（一一映射）而且是互逆的. 其次，根据性质 (2)，ϕ 的某些值只取决于 G 的本质而不取决于子群 U. 重新考虑固定的 s 和全体 $g\in G$. 这些 g 可以分成两个类 $C(s)$ 和 $C^*(s)$，使得

$$g\in C(s)，必要而且只要 gs\in G,$$

$$g\in C^*(s)，必要而且只要 gs\notin G.$$

设 $N(s)$ 是类 $C(s)$ 的基数，$M(s)$ 是类 $C^*(s)$ 的基数. 于是

$$N(s)+M(s)=N,$$

这里 N 是 G 的基数. 同理，设

$$g\in C(s^{-1})，必要而且只要 gs^{-1}\in G,$$

$$g\in C^*(s^{-1})，必要而且只要 gs^{-1}\notin G,$$

再用 $N(s^{-1})$ 表示 $C(s^{-1})$ 的基数，$M(s^{-1})$ 表示 $C^*(s^{-1})$ 的基数，我们有

$$N(s^{-1})+M(s^{-1})=N.$$

现在如果 g_i 和 g_j 是使 $g_is=g_j$ 因而 $g_js^{-1}=g_i$ 的 g，则 $g_i\in C(s)$ 和 $g_j\in C(s^{-1})$. 这个关系确立了 $C(s)$ 和 $C(s^{-1})$ 之间的一一对应，因而

$$N(s)=N(s^{-1}).$$

当 N 是有限的时，由此还能得出

$$M(s)=M(s^{-1}).$$

但是当N是无限的时，不能由此得出 $M(s)=M(s^{-1})$ 对于任意的施赖尔组成立. 例如取 $1, s, s^2, \cdots, s^i, \cdots$. 这时 $M(s)=1, M(s^{-1})=0$. 另一方面，如果对于给定的G存在一个 ϕ，则 $\pi(s)$ 是一个置换，它不仅把 $C(s)$ 映到 $C(s^{-1})$，而且把 $C^*(s)$ 映到 $C^*(s^{-1})$. 因此 $M(s)=M(s^{-1})$ 是ϕ存在的必要条件.

定理 7.2.6. 给了施赖尔组 G，使得对于每个生成元素 s 都有 $M(s)=M(s^{-1})$. 那么就能找到一个函数 $\phi(gs^{\varepsilon})$满足下列三个性质:

1) $\phi(gs^{\varepsilon})$ 是一个 $g\in G$.

2) 如果 $gs^{\varepsilon}\in G$，则 $\phi(gs^{\varepsilon})=gs^{\varepsilon}$.

3) $\phi[\phi(gs^{\varepsilon})s^{-\varepsilon}]=g$.

要得出最广的 ϕ，只要对于每个 s，令:

i) $\phi(gs)=gs$，假如 gs 是一个 g.

ii) 对于不是一个 g 的 gs，以任何方式取 $\phi(gs)$，只要使 $\pi(s): g\to\phi(gs)$ 是G的置换.

iii) 在对于所有 g 都定义了 $\phi(gs)$ 以后，定义 $\phi(gs^{-1})$，使 $\pi(s^{-1}): g\to\phi(gs^{-1})$ 是 $\pi(s)$ 的逆.

证明. 对于所有生成元素 s，在G上给了条件 $M(s)=M(s^{-1})$，这个定理不仅断定 $\phi(gs^{\varepsilon})$ 存在，而且描述了什么是最普遍的构造(如果这种构造有效的话). 因此我们必须证明这种构造的有效性. 对于给定的 s，显然有:

1) $\phi(gs)$ 是一个 g.

2) 如果 gs 是一个 g，则 $\phi(gs)=gs$.

如果对于某个 g_i，我们有 $g_is=g_j\in G$，则我们已经令 $\phi(g_is)=g_j$. 这时 $g_js^{-1}=g_i$. 因而在 $g\to\phi(gs)$ 下我们把类 $C(s)$映到类 $C(s^{-1})$ 上. 于是剩下有 $M(s)$ 个 g 被映成剩下的 $M(s^{-1})$ 个 g. 因为 $M(s)=M(s^{-1})$，所以可能存在一个一一对应把

$C^*(s)$ 映到 $C^*(s^{-1})$ 上，即对于 $g\in C^*(s)$ 有 $g\rightleftarrows g'\in C^*(s^{-1})$. 我们令 $g'=\phi(gs)$. 于是 $\pi(s): g\rightleftarrows\phi(gs)$ 就是一个一一对应把 $C(s)$ 映到 $C(s^{-1})$ 上和把 $C^*(s)$ 映到 $C^*(s^{-1})$ 上. 现在因为 $\pi(s)$ 是置换，所以我们只要取 $\pi(s^{-1}): g\rightleftarrows\phi(gs^{-1})$ 作为 $\pi(s)$ 的逆，我们就定义了 $\phi(gs^{-1})$ 的值. 这里 $\phi(gs^{-1})$ 显然是一个 g. 其次，因为 $\pi(s)$ 把 $C(s)$ 映到 $C(s^{-1})$ 上，所以：

3) 如果 gs^{-1} 是一个 g，则 $\phi(gs^{-1})=gs^{-1}$. 因此对于所有 $g\in G$ 以及 s 和 s^{-1}，性质 (1) 和 (2) 都成立. 最后因为 $\pi(s)$ 和 $\pi(s^{-1})$ 是互逆的置换；所以性质 (3) $\phi[\phi(gs^{\epsilon})s^{-\epsilon}]=g$ 也成立.

在定理 7.2.5 和 7.2.6 里，置换 $\pi(s)$ 都占有中心的地位. 设 $g=a_1a_2\cdots a_t$，我们发现置换 $\pi(a_1)\pi(a_2)\cdots\pi(a_t)$ 把 1 变成 g，因而置换 $\pi(s)$ 生成一个在 g 上传递的群. 这些置换唯一地决定子群 U，这是我们现在要证明的.

定理 7.2.7. 设 F 是自由生成组 S 上的自由群. 设对于每个 $s\in S$ 都给定一个置换 $\pi(s)$，它是在符号 $1, y_2, \cdots, y_i, \cdots$ 上的置换，而且由 $\pi(s)$ 生成的群是在这些符号上传递的. 对于 F 的每个元素 $f=a_1a_2\cdots a_t$，结合着置换 $\pi(f)=\pi(a_1)\pi(a_2)\cdots\pi(a_t)$. 那么使 $\pi(f)$ 不变 1 的元素 f 组成一个子群 U. 如果 $g_1=1, g_2, \cdots, g_i, \cdots$ 是由 U 的左傍系代表组成的施赖尔组，我们可以把这些 g 与符号 y_i 结合起来，当 $\pi(g_i)$ 把 1 变成 y_i 时，令 $g_i\rightleftarrows y_i$. 在这种方式下，y_i 上的 $\pi(s)$ 是同构于定理 7.2.5 和 7.2.6 中 g_i 上的 $\pi(s)$ 的置换[1].

证明. 明显地，$\pi(f)$ 不变 1 的那些 f 组成 F 的一个子群

---

1) 注意作者在这里既用 $\pi(s)$ 表出个别的置换，也用它表出作为已知群的置换表示的整个置换群.——译者

U. 根据定理 5.3.1，我们可以把置换 $\pi(f)$ 看作 F 在 U 的傍系上的表示，它把 1 换成 U 而把那些 y 换成 U 的其他左傍系．因此每个 y_i 唯一地对应于某个左傍系 Ug_i，这里 $\pi(g_i)$ 把 1 变成 y_i．在这个表示下，$\pi(s)$ 把傍系 Ug 变成 Ugs，它是与 $U\,\phi(gs)$ 相同的傍系．因此，如果我们把傍系 Ug_i 换成它的代表 g_i，置换 $\pi(s)$ 就变成定理 7.2.5 和 7.2.6 的置换 $\pi(s)$，因而我们完全地确立了那些 y 上的原来的置换与施赖尔组 G 上的置换的置换同构．

对于有限生成的自由群内有限指数的子群 U，我们可以给出 U 的生成元素数和它们的总长度的一些确定的值．

定理 7.2.8. 设 $U = U[G,\ \phi(gs^{\epsilon})]$ 是自由群 F_r 的有限指数 n 的子群，F_r 有 r 个自由生成元素 $s_1, s_2, \cdots, s_r$. 那么

1) U 是在 $1+n(r-1)$ 个自由生成元素上的自由群．

2) 如果 L 是施赖尔组 G 的总长度，则 U 的自由生成元素 $u = gs\phi(gs^{-1}) \neq 1$ 的总长度是 $K = (2L+n)r - 2L$.

证明. 我们已经证明 U 的自由生成组由下列元素组成：

$$u_{ia} = g_i s_a \phi(g_i s_a)^{-1},\ i = 1, \cdots, n;\ a = 1, \cdots, r,$$

它们都不等于单位元素．其次根据引理 7.2.3，u_{ia} 或是写成简化形式的，或者等于单位元素．现在

$$\sum_{i=1}^{n} L(g_i) + L(s_a) + L[\phi(g_i s_a)] = 2L + n.$$

因为对于固定的 s_a，$\phi(g_i s_a)$ 是 g 的一个置换．因此在消去之前我们有总长度为 $r(2L+n)$ 的 nr 个 u．因而我们必须从这些总长度分别减去等于单位元素的 u_{ia} 数和对于这些 u 计算的长度 $L(g_i) + L(s_a) + L(g_i s_a)$．$u_{ia}$ 什么时候等于单位元素呢？现在 g_i，s_a 和 $\phi(g_i s_a)^{-1}$ 是写成简化形式的．因此要是有消去(于是根据引理 7.2.3 就有 $u_{ia} = 1$)，必要而且只要

s_a能与 g_i 或 $\phi(g_is_a)^{-1}$消去．在第一种情况下，g_i 以 s_a^{-1} 结尾：$g_i = g_js_a^{-1}$，这里 $g_j \in G$ 是写成简化形式的．在第二种情况下，$\phi(g_is_a) = g_k$ 以 s_a 结尾，因而实际上有 $g_k = gs_a$．因此对于给定的 s_a 说，等于单位元素的 u 的个数等于以 s_a 或 s_a^{-1} 结尾的 g 的个数．但是除 $g=1$ 外，每个 g 若以某个 s_a 或 s_a^{-1} 结尾，因而在这步骤下恰好计算一次．因此一共有 $n-1$ 个 u 等于单位元素，由此可知还剩下 $nr-(n-1)=n(r-1)+1$ 个 u 是自由生成元素．关于长度的情况怎样呢？首先，如果 $g_i = g_js_a^{-1}$，则 $\phi(g_is_a) = g_j$，因而 $L(g_i)+L(s_a)+L[\phi(g_is_a)] = 2L(g_i) = 2L(g_js_a^{-1})$．其次，如果 $g_is_a = g_k$，则 $L(g_i)+L(s_a)+L[\phi(g_is_a)] = 2L(g_is_a)$．因而对于给定的 s_a，包括 $u_{ia}=1$ 在内，我们有以 s_a 或 s_a^{-1} 结尾的每个 g 的长度的两倍．因此对于所有的 s_a，包括等于 1 的 u 在内，我们有除 $g=1$ 外的每个 g 的长度的两倍．但是 $L(1)=0$，因而必须恰好减去 $2L$，剩下 $(2L+n)r-2L$ 正是U的自由生成元素的总长度．

最后，利用定理 7.2.7，我们可以递归地计算在 F_r 内指数为 n 的子群的个数．

定理 7.2.9. F_r 内指数为 n 的子群的个数 $N_{n,r}$ 可以由下列递归公式给出：$N_{1r}=1$，

$$N_{n,r} = n(n!)^{r-1} - \sum_{i=1}^{n-1}(n-i)!^{r-1}N_{i,r}.$$

证明． $N_{1r}=1$ 只不过断定 F_r 是它自己的唯一的指数为 1 的子群．

取文字 $1, x_2, \cdots, x_n$ 上的 r 个置换 $P_1, \cdots, P_r$．一般说来 $P_1, \cdots, P_r$ 并不生成在全体 $1, x_2, \cdots, x_n$ 上传递的群．设包含 1 的传递组是 $1, b_2, \cdots, b_i$．不考虑其余的文字，我

们可以取 $1, b_2, \cdots, b_t$ 上的置换作为 $\pi(s_1), \cdots, \pi(s_r)$, 然后根据定理 7.2.7, 这些置换决定唯一的指数为 t 的子群. 剩下的 $n-t$ 个文字在 $P_1, \cdots, P_r$ 中出现有 $[(n-t)!]^r$ 种方式. 再有如果我们把 $1, b_2, \cdots, b_t$ 换成任何别的组合 $1, c_2, \cdots, c_t$ 而且令剩下的 $n-t$ 个文字以任意方式出现, 则决定的是同一个子群. 因而与指数为 t 的同一个子群结合总共有

$$(n-1)(n-2)\cdots(n-t+1)[(n-t)!]^r = (n-1)![(n-t)!]^{r-1}$$

种不同的置换 $P_1, \cdots, P_r$. 因此, 以对应于 $P_1, \cdots, P_r$ 所结合的子群的指数来计算 $P_1, \cdots, P_r$ 的 $(n!)^r$ 个可能的选取,

$$\sum_{t=1}^{n}(n-1)![(n-t)!]^{r-1}N_{t,r} = (n!)^r.$$

用 $(n-1)!$ 去除这个式子而且改变和式的上下限为 1 到 $n-1$, 我们就得到定理中的公式.

7.3. 自由群的子群的自由生成元素. 臬尔逊方法

在 § 7.2 中通过子群 U 在自由群 F 内的傍系来研究 F 的子群的性质. 在本节中我们将要更直接地来探讨 U 的元素.

设 $A=\{a_i\}$ 是自由群 F 内具有指标 i 的集合 I 的元素集合, 再设集合 A 由它所生成的群的自由生成元素组成, 我们把这个群记做 $[A]$. 对于元素 $f\in A$, 我们用 $L_A(f)$ 表示把 f 写成以 a 和它们的逆表出的简化字的长度.

设集合 X 是自由群 F 的自由生成元素的集合. 那么我们说 F 的元素集合 A 具有相对于生成元素集合 X 的臬尔逊性质, 必要而且只要

1) $A\cap A^{-1}=0$ (A^{-1} 是 A 的元素的逆的集合).

2) 如果 $a, b \in A \cup A^{-1}$，则从 $L_X(ab) < L_X(a)$ 得出 $b = a^{-1}$.

3) 如果 $a, b, c \in A \cup A^{-1}$，则从 $L_X(abc) \leqslant L_X(a) - L_X(b) + L_X(c)$ 得出 $b = a^{-1}$ 或 $b = c^{-1}$.

定理 7.3.1. 如果集合 A 具有相对于 F 的自由生成元素集合 X 的臬尔逊性质，则 A 由它所生成的子群 $[A]$ 的自由生成元素组成．臬尔逊性质等价于在 A 中存在中心有效因子．

证明．只要证明臬尔逊性质等价于中心有效因子的存在就成了，因为根据定理 7.2.2，从这就能得出 A 由 $[A]$ 的自由生成元素组成.

假定 A 具有臬尔逊性质．那么根据性质(2),如果 $b \neq a^{-1}$，则 $L_X(ab) \geqslant L_X(a)$ 而且 $L_X(b^{-1}a^{-1}) \geqslant L_X(b^{-1})$，因而 $L_X(ab) \geqslant L_X(b)$．如果在 ab 的简化形式中，有一个因子 b 的多于一半与 a 消去，则我们将有 $a = uv^{-1}$，$b = vw$，$L_X(v) > L_X(w)$ 而且 $L_X(ab) = L_X(uw) < L_X(u) + L_X(v) = L_X(a)$．因此这不可能发生，即在 ab 的简化形式中最多有 a 或 b 的一半被消去．于是对于奇数长度的元素，它的中心项可以取作有效因子．如果 b 是偶数长度的，设想 b 的前一半 v 在乘积 $ab\,(b \neq a^{-1})$ 中可能被消去．同样，如果 b 的后一半 w 在乘积 $bc\,(b \neq c^{-1})$的简化形式中被消去，则我们有 $a = uv^{-1}$，$b = vw$，$c = w^{-1}z$，因而 $L_X(abc) = L_X(uz) \leqslant L_X(u) + L_X(z) = L_X(a) - L_X(b) + L_X(c)$，这与臬尔逊性质的第三个要求矛盾． 因为这不能发生，所以 b 的一半，不论是 v 或 w，在任何乘积内都不能消去，因而 b 的两个中心项中属于这一半的一个可以取作它的中心因子． 因此臬尔逊性质导出中心有效因子的存在． 反之，如果对于有性质 $A \cap A^{-1} = 0$ 的集合 A，中心有效因子存在，则当 $b \neq a^{-1}$ 时在 ab 内最多有 b 的一半与 a 内同样

多项消去；因而 $L_X(ab) \geq L_X(a) + L_X(b) - 2 \cdot \frac{1}{2} L_X(b) = L_X(a)$，引出第二个要求．其次在乘积 abc 中，当 $b \neq a^{-1}$，$b \neq c^{-1}$ 时，a 和 b 之间以及 b 和 c 之间的消去终止在 b 的有效因子之前；因而 $L_X(abc) > L_X(a) + L_X(b) + L_X(c) - 2L_X(b)$，这就是第三个要求．不难证明单是第三个要求就等价于有效因子的存在．对于给定的 b，取 $a \neq b^{-1}$ 为能在 b 的左边消去最多个项的元素，而且取 $c \neq b^{-1}$ 为能在 b 的右边消去最多个项的元素． 第三个要求断定不会全部 b 都消去，于是剩下的项就可以取作 b 的有效因子．

定理 7.3.2. 给了具有已知自由生成元素组 X 的自由群 F 的元素 $\beta_1, \cdots, \beta_m$ 的有限集合 B．经过有限次下列类型的改变：

类型 1：删去一个 $\beta_i = 1$，

类型 2：把一个 β_i 换成 β_i^{-1}，

类型 3：把一个 β_i 换成 $\beta_i\beta_j$，$i \neq j$，

我们可以把集合 B 换成另一个集合 A：$\alpha_1, \cdots, \alpha_n$，$n \leqslant m$，使得 A 与 B 生成同一个子群，而且 A 具有相对于 X 的巢尔逊性质．因此 A 是使 $[A] = [B]$ 的自由生成元素集合．

证明． 显然每一次改变都把一个集合换成生成同一个群的集合．第一类型减去元素的个数，第二和第三类型不变动元素个数．我们看到第二和第三类型改变的联合可以把 β_i 换成 $\beta_i^\epsilon \beta_j^\eta$ 或 $\beta_j^\eta \beta_i^\epsilon$，$\epsilon = \pm 1$，$\eta = \pm 1$，而且保留其余的 β 不变

如果有两个 β 相等或互逆，我们可以进行改变而把 β 换成 1，然后删去这个 1．这样就减少 β 的个数，而且这最多有 m 次．如果对于 $a, b \in B \cup B^{-1}$，$b \neq a^{-1}$，我们有 $L_X(ab) < L_X(a)$，则我们不能有 $b = a$，因为总有 $L_X(a^2) \geqslant L_X(a)$．因此我们可以把 $\beta = a^\epsilon$ 换成 ab，因而就减少了全部 β 的总长

度．因此只可能有有限步这种改变，所以只要经过有限步就能使臬尔逊性质的要求（1）和（2）满足．要满足第三个要求是较为困难的．

不论集合 X 是否无限的，生成元素 X 中在 β 中出现的子集 Y 总是有限的．我们把 F 中由 Y 生成的元素按长度排成表，同一长度元素的顺序是任意地排定的．因为只有有限个同一长度的元素，所以在这个表的每个元素之前只有有限个元素．

如果 β 有偶数长度 $2k$，把 β 写成 $\beta=\gamma\delta^{-1}$，这里 γ 和 δ 是有同样长 k 的．如果 $\beta\neq 1$，则 $\delta\neq\gamma$．因为 $\beta^{-1}=\delta\gamma^{-1}$，必要时把 β 换成 β^{-1}，总可以使得这两半 γ 和 δ 中，前一半在表中排在后一半之前．如果 $\beta_i=\gamma\delta^{-1}$ 而且 β_j 以 δ 的各项开始，$\beta_j=\delta z$，则我们把 β_j 换成 $\beta_i\beta_j=\gamma z$．同理，如果 β_k 以 δ^{-1} 结尾，则我们把 $\beta_k=w\delta^{-1}$ 换成 $\beta_k\beta_i^{-1}=w\gamma^{-1}$．因此我们可以改写 β，使得在 $\beta_i=\gamma\delta^{-1}$ 时，没有其他 β 以 δ 开始或以 δ^{-1} 结尾．因为我们把一系列的 δ 换成同样长度但是在表中较前的 γ，所以这个过程在有限步以后就要终止．必须注意如果我们从偶数长度的最短的 β 开始，然后继续处理偶数长度的较长的 β，则这个过程也将以有限步而终止．在处理同一长度的 β 时，我们逐步地把字的一半换成字的较前的一半，因而我们在有限步后将达到一个终止点．在处理长度大于 $\beta_i=\gamma\delta^{-1}$ 的 β 时，在其中任何一个都不会有开始部分 δ 和结尾部分 δ^{-1}．自然地，如果在任何一步上条件 $A\cap A^{-1}=0$ 或 $L_X(ab)\geqslant L_X(a)$ 违反了，则我们作适当的改变，或者减少 β 的个数，或者减少它们的总长度，再开始更换字的一半，这不会变动 β 的个数和长度．因此经过有限步改变这个过程就终止了，这时产生一个集合 $A:\alpha_1,\cdots,\alpha_n$，$n\leqslant m$．我们断定集合 A 具有相对于 X 的臬尔逊性质．$A\cap A^{-1}=0$ 和 $L_X(ab)\geqslant$

$L_X(a)$, $b \neq a^{-1}$, $a, b \in A \cup A^{-1}$ 当然成立，因为否则我们就能减少 α 的个数或者总长度. 现在考虑乘积 abc, $b \neq a^{-1}$, $b \neq c^{-1}$. 如果 b 有奇数长度 $2k+1$, b 的最多前 k 项与 a 消去而且最多后 k 项与 c 消去；因而 $L_X(abc) > L_X(a) - L_X(b) + L_X(c)$ 成立. 如果 b 有偶数长度，则 b 有形状 $\gamma\delta^{-1}$ 或 $\delta\gamma^{-1}$, 这里 γ 在 δ 之前. 因为第二个性质成立，所以 b 最多有一半与 a 消去，又最多有一半与 c 消去. 但是 a 不能以 δ^{-1} 结尾，c 不能以 δ 开始，所以 b 的不论是 δ 或 δ^{-1} 的一半都不能完全消去；因而 b 本身不能整个消去，于是 $L_X(abc) > L_X(a) - L_X(b) + L_X(c)$, 这就对 A 证明了臬尔逊性质的第三个要求.

定理 7.3.3. 两个自由群同构，必要而且只要它们的自由生成元素的基数相同. 具有有限的 r 个生成元素的自由群 F_r 是由生成它的任何 r 个元素的集合自由生成的.

证明. 设 F_X 和 F_Y 是分别在自由生成元素集合 X 和 Y 上的自由群.

如果 X 和 Y 的基数相同，则在 X 和 Y 之间存在一一对应，它可以推广成 F_X 和 F_Y 之间的一一对应，这显然是同构.

反之，假定 F_X 和 F_Y 是同构的. 那么 F_X 和 F_Y 具有同样个数指数为 2 的子群. 指数为 2 的子群是到 2 阶群上的同态的核. 这样一个同态由映到单位元素上的生成元素集合唯一决定. 因而在生成元素集合 Z 上的自由群 F_Z 的子群的个数是 Z 的非空子集的个数. 当 Z 是无限集时这数是不可数的，而当 Z 包含有限的 r 个元素时它是 $2^r - 1$. 因此，如果 F_X 和 F_Y 同构，则 X 和 Y 或者都是无限的，或者都是有限的，而且在后一情形 X 和 Y 有同样个数的元素. 如果 X 和 Y 是无限的，则 F_X 和 F_Y 分别与 X 和 Y 有相同的基数. 而因为 F_X 和 F_Y 有相同的基数，所以 X 和 Y 也是如此.

现在假定在 $X: x_1, x_2, \cdots, x_r$ 上的自由群 F_r 也是由 $\beta_1, \beta_2, \cdots, \beta_r$ 生成的群. 于是根据定理 7.3.2,经过若干次(关于 $\beta_1, \cdots, \beta_r$) 类型 1, 2, 3 的改变,我们将得出由 $\alpha_1, \cdots, \alpha_s$ ($s \leqslant r$) 自由生成的 F_r. 但是那时我们必须有 $s = r$,因而不会用到类型 1 的改变. 我们可以直接验证, 如果有一个类型 2 或 3 的改变使集合 B 成为集合 B', 则当 B 或 B' 中有一个由自由生成元素组成时,另一个也是如此. 因此,因为 $\alpha_1, \cdots, \alpha_r$ 是 F_r 的自由生成元素,所以 $\beta_1, \cdots, \beta_r$ 也是 F_r 的自由生成元素.

这就证明了上述定理,但是我们还可以得到关于 $\alpha_1, \cdots, \alpha_r$ 的更确切的知识. α_i 具有臬尔逊性质, 因而具有中心有效因子 (定理 7.3.1). 其次对于每个 x_i, $i = 1, \cdots, r$, $x_i = \gamma_1, \cdots \gamma_m$,这里 γ 是一个 α 或它的逆,而且 $\gamma_i \gamma_{i+1} \neq 1$. 现在这些 γ 的乘积在以它的简化形式写出时包括了每一个中心有效因子. 因此只可能有一个 γ 而且它必须等于 x_i. 因而每个 x_i 是一个 α_j 或 α_j^{-1}. 因此, 如果我们进一步进行第二类型的改变, 则这些 α 明显地是以某个次序排列的 $x_1, \cdots, x_r$. 于是,不考虑顺序,我们就能知道如何可以从 $x_1, \cdots, x_r$ 得到 F_r 的任何自由生成元素组 $\beta_1, \cdots, \beta_r$. 而这是说我们有了关于 F_r 的自同构的知识.

定理 7.3.4. 在有限的 r 个生成元素 X 上的自由群 F_r 的全体自同构由下列自同构生成:

1) $P_{ij}: x_i \to x_j,\ x_j \to x_i,\ x_k \to x_k,\ k \neq i, j$.

2) $V_i: x_i \to x_i^{-1},\ x_j \to x_j,\ j \neq i$.

3) $W_{ij}: x_j \to x_i x_j,\ i \neq j,\ x_k \to x_k,\ k \neq j$.

证明. 这些显然都是 F_r 的自同构,因为它们都把 X 换成生成 F_r 的一组 r 个元素. 我们必须证明 F_r 的任意自同构都能表成这些自同构的乘积. 我们刚才证明过 F_r 的最一般的

自同构从把 $X:x_1, \cdots, x_r$ 换成生成元素组 $B:\beta_1, \cdots, \beta_r$ 而得到，而且集合 B 与 X 由有限步的逐次改变联系着，

$$B = B_1, B_2, \cdots, B_{N-1}, B_N = X,$$

这里 B_i 从 B_{i+1} 经过定理 7.2.3 的类型 2 或 3 的改变而得到，$i = 1, \cdots, N-2$，而从 B_{N-1} 到 B_N 的改变则是集合 X 的一个置换，因而是对换 P_{ij} 的乘积(§ 5.4)．因而从 B_{i+1} 到 B_i 的每个改变 $(i = 1, \cdots, N-2)$ 是以 B_{i+1} 的元素表示的一个自同构 V_i 或 W_{ij}．我们必须证明它们可以用以 X 的元素表示的自同构 V_i 或 W_{ij} 来表出．

现在设

$$Y: y_1, \cdots, y_r,$$
$$Z: z_1, \cdots, z_r,$$
$$W: w_1, \cdots, w_r$$

是 F_r 的三组自由生成元素，这里

1) $z_i = y_i^{-1}, \ z_j = y_j, \ j \neq i$, 或
2) $z_j = y_i y_j, \ z_k = y_k, \ k \neq j$, 而且
3) $w_m = z_m^{-1}, \ w_n = z_n, \ n \neq m$, 或
4) $w_n = z_m z_n, \ w_t = z_t, \ t \neq n$.

这时把 Y 换成 Z 是 Y 的一个 V 或 W 自同构，把 Z 换成 W 是 Z 的一个 V 或 W 自同构．我们必须证明 (3) 或 (4) 可以用 Y 上的 V 和 W 自同构表出．这包括几种情形都是比较简单的．这里只给出两种最困难的情形．假定我们有 (2) $z_j = y_i y_j$ 和 (3) $w_m = z_m^{-1}$, $m = j$．我们必须把自同构 (3) 表示成把 $y_i y_j$ 换成 $y_j^{-1} y_i^{-1}$ 而且保留 $y_k \ (k \neq j)$ 不变．这相当于把 y_j 换成 $y_i^{-1} y_j^{-1} y_i^{-1}$ 而且保留全体其余的 y 不变．但是这是乘积

$$y_j \to y_i^{-1} y_j \to y_i^{-1} y_j^{-1} \to y_i^{-1} y_j^{-1} y_i^{-1},$$

它是 $W_{ij}^{-1}(y) V_j(y) W_{ij}(y)$．其次，假定我们有 (2) $z_j = y_i y_j$ 和 (4) $w_n = z_m z_n$, $m = j$, $n = i$．这时自同构 (4) 把 $z_i =$

y_iy_j 换成 y_iy_j 和把 $z_i=y_i$ 换成 $y_iy_jy_i$ 而且保留全体其他的 $z_k=y_k$ 不变. 这相当于代换

$$y_i \to y_iy_jy_i$$
$$y_j \to y_i^{-1}.$$

但是这是乘积

$$y_i \to y_i \to y_jy_i \to y_iy_jy_i,$$
$$y_j \to y_i^{-1}y_j \to y_i^{-1} \to y_i^{-1}.$$

即是 $W_{ij}^{-1}(y)$, $W_{ji}(y)$, $W_{ij}(y)$. 因此 z 上的每一个V或W自同构可以用 y 上的V和W自同构表出. 我们现在可以利用对N的归纳法来证明定理了. 从 B_{N-1} 到 B_1 的代换可以归纳地假设为在 B_{N-2} 的生成元素上的一些V和W的乘积. 然后把 B_{N-1} 看做集合 Y,把 B_{N-2} 看做集合Z,我们可以把从 B_{N-2} 到 B_1 的代换用集合 B_{N-1} 上的一些V和W表出. 从 B_{N-1} 到 B_{N-2} 的代换是 B_{N-1} 上的一个V或W. 因此从 B_{N-1} 到 B_1 的代换是 B_{N-1} 上的一些V和W的乘积,而且因为 B_{N-1} 只不过是X的一个置换,所以它们也是X上的一些V和W的乘积. 这就证明了定理.

如果A是具有相对于 F_X 的自由生成元素组X的臬尔逊性质的集合,则A在很多方面可以看作[A]的"最短的"生成元素组.

定理 7.3.5. 如果A具有相对于X的臬尔逊性质而且

$$f=a_1a_2\cdots a_t,\quad a_i\in A\cup A^{-1},\quad a_ia_{i+1}\neq 1,$$

则

$$L_X(f)\geqslant \frac{1}{2}L_X(a_1)+t-2+\frac{1}{2}L_X(a_t),$$

而且

$$L_X(f)\geqslant L_X(a_i\cdots a_j),\ 1\leqslant i\leqslant j\leqslant t.$$

其次,如果X是有限的而且A的元素按长度增大的次序排列

$$\alpha_1, \alpha_2, \cdots, \alpha_i, \cdots,$$

又如果

$$\beta_1, \beta_2, \cdots, \beta_i, \cdots$$

是 A 的任意自由生成元素组，也按长度增大的次序排列，则

$$L_X(\beta_n) \geqslant L_X(\alpha_n), \quad n = 1, 2, \cdots.$$

证明. 在 $f = a_1 a_2 \cdots a_t$ 内每个 a_i 有一个中心因子，它在 f 的简化形式中未被消去. 因此在 f 的简化形式中，至少 a_1 的前半，$a_2, \cdots, a_{t-1}$ 的中心因子和 a_t 的后半会留下，这就得出 $L_X(f) \geqslant \frac{1}{2} L_X(a_1) + t - 2 + \frac{1}{2} L_X(a_t)$. 在 $a_1 \cdots a_{t-1} a_t$ 的简化形式中，在 $a_1 \cdots a_{t-1}$ 的简化形式和 a_t 之间的消去包括 a_{t-1} 的 k 项和 a_t 的 k 项，这里 $k \leqslant \frac{1}{2} L_X(a_{t-1})$, $k \leqslant \frac{1}{2} L_X(a_t)$, 因为它们的中心因子都不会消去. 因而

$$L_x(f) = L_X(a_1 \cdots a_{t-1}) + L_X(a_t) - 2k.$$

但是 $2k \leqslant L_X(a_t)$，所以 $L_X(a_1 \cdots a_t) \geqslant L_X(a_1 \cdots a_{t-1})$. 同理 $L_X(a_1 \cdots a_t) \geqslant L_X(a_2 \cdots a_t)$. 重复这个论证，每次从这一端或那一端减少一个 a，就能得出 $L_X(a_1 \cdots a_t) \geqslant L_X(a_i \cdots a_j)$.

如果 X 是有限的，则只有有限个元素具有同一个已知长度，因此以递增的长度排列 A 可以穷尽整个集合. 设这个排列是 $\alpha_1, \alpha_2, \cdots, \alpha_i, \cdots$. 设对于第二个生成元素组，这排列是 $\beta_1, \beta_2, \cdots, \beta_i, \cdots$. 设 $\beta_1(\alpha), \cdots, \beta_n(\alpha)$ 是由自由生成元素组 A 表出的前 n 个 β，再设 α_r 是在这些表达式中出现的最后一个 α. 我们可以断定 $r \geqslant n$. 要是我们否定这个结论而假定 $r < n$. 那么对 $[A]$ 的换位子子群[1] K 取模，我们有

$$\beta_1 \equiv \alpha_1^{e_{11}} \cdots \alpha_r^{e_{1r}} \pmod K,$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

1) 参看本书 § 9.2 关于换位子子群的性质.——译者

$$\beta_n \equiv \alpha_1^{e_{n1}} \cdots \alpha_r^{e_{nr}} \pmod{K}.$$

当 $r < n$ 时必定存在[1]整数 $u_1, \cdots, u_t$ 不全是零，使得

$$e_{11}u_1 + \cdots + e_{n1}u_n = 0,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$e_{1r}u_1 + \cdots + e_{nr}u_n = 0.$$

于是 $\beta_1^{u_1}\cdots\beta_n^{u_n} \in K$，这里 $u_1, \cdots, u_n$ 不全是零，这与这些 β 是 $[A]$ 的自由生成元素的假设矛盾．因此 $r \geqslant n$．设 a_r 事实上在某个 $j \leqslant n$ 的 $\beta_j(\alpha)$ 内出现．那么根据定理的第一部分，$L_X(\beta_j) \geqslant L_X(\alpha_r)$．但是 $L_X(\beta_n) \geqslant L_X(\beta_j)$ 而且 $L_X(\alpha_r) \geqslant L_X(\alpha_n)$，这是因为 $r \geqslant n$，于是 $L_X(\beta_n) \geqslant L_X(\alpha_n)$．

习　　题

1．设 F 是由 x 和 y 生成的自由群．证明 F 中包含 x^2yxy^{-1} 的完全不变子群或是 F 自己，或者在 F 内的指数是 9．

2．设 F 是具有两个生成元素的自由群．找出它的指数为 3 的所有子群．

3．设 F 是由三个元素 a，b，c 生成的自由群．找出由 F 的所有元素的平方生成的指数为 8 的子群的一个自由生成元素组．

4．设 $A_1, A_2, \cdots, A_m$ 是自由群的以简化形式写出的元素，其中没有 1，但是 $A_1A_2\cdots A_m = 1$．证明存在某个 i，使 A_i 在乘积 $A_{i-1}A_iA_{i+1}$ 中整个被消去．

5．在自由群 F 内给了简化字 $g = a_1a_2\cdots a_t \neq 1$．证明 F 具有指数为 $t+1$ 的子群 H，使得 $g \notin H$．（提示：取 H 的傍系代表为 $1, a_1, a_1a_2, \cdots, a_1a_2\cdots a_t$．）

6．证明，如果 $g = g(x_1, \cdots, x_r)$ 是以生成元素 $x_1, \cdots, x_r$ 表出的字，它在以 $x_1, \cdots, x_r$ 作为自由生成元素的自由群内不是单位元素，则就存在由元素 $x_1, \cdots, x_r$ 生成的有限群 G，使 g 在这群中也不是单位元素．（利用本章习题 5 和第五章习题 1．）

1）参看 Birkhoff and MacLane[1]，第 48 页．

第八章　格和合成序列

8.1. 偏序集合

定义. 偏序集合是元素体系 S，在其中对于 S 的某些对元素定义了关系 $a \supseteq b$（读做"a 包含 b"），使得

$P1$. $a \supseteq a$.

$P2$. 如果 $a \supseteq b$ 和 $b \supseteq c$，则 $a \supseteq c$.

$P3$. 如果 $a \supseteq b$ 和 $b \supseteq a$，则 $a = b$.

定义. 偏序集合 S 的子集 T 的上界是指对于 T 的每个 t 都有 $x \supseteq t$ 的 S 的元素 x. 同理，子集 T 的下界是指对于 T 的每个 t 都有 $t \supseteq y$ 的 y.

定义. S 的子集 T 的最小上界（$l.u.b.$）是指满足下列条件的元素 x:

1）x 是 T 的一个上界.

2）如果 z 是 T 的任何上界，则 $z \supseteq x$.

同理，最大下界（$g.l.b.$）是指满足下列条件的元素 y:

1）y 是 T 的一个下界.

2）如果 z 是 T 的任何下界，则 $y \supseteq z$.

一般地说，子集 T 不一定具有最小上界和最大下界. 但是如果 T 具有最小上界 x，则这是唯一的，因为根据定义，两个最小上界必须彼此包含，因而根据 $P3$，它们必须相等. 对于最大下界有相同的结论.

如果偏序集合 S 还满足

$P4$. 对于每一对 a 和 b，或者 $a \supseteq b$，或者 $b \supseteq a$.

则我们说 S 是全序集合或链.

我们用 $b \subseteq a$ 表示 $a \supseteq b$. 我们还用 $a \supset b$ 表示 $a \supseteq b$ 而 $a \neq b$. 同理, $b \subset a$ 表示 $a \supset b$. 另一个有用的记号是 $a > b$ (读做"a 盖住 b"),它表示 $a \supset b$ 而且从 $a \supseteq x \supseteq b$ 得出 $a = x$ 或 $x = b$. 再有 $b < a$ 表示 $a > b$.

例. 设 S 是一组元素 a, b, c, d, e, f, 它们的包含关系由图表出. 当 x 在 y 之上而且有线段连结它们时就说 $x \supseteq y$. 这时由 c 和 d 组成的子集没有上界, 它有两个下界但是没有最大下界.

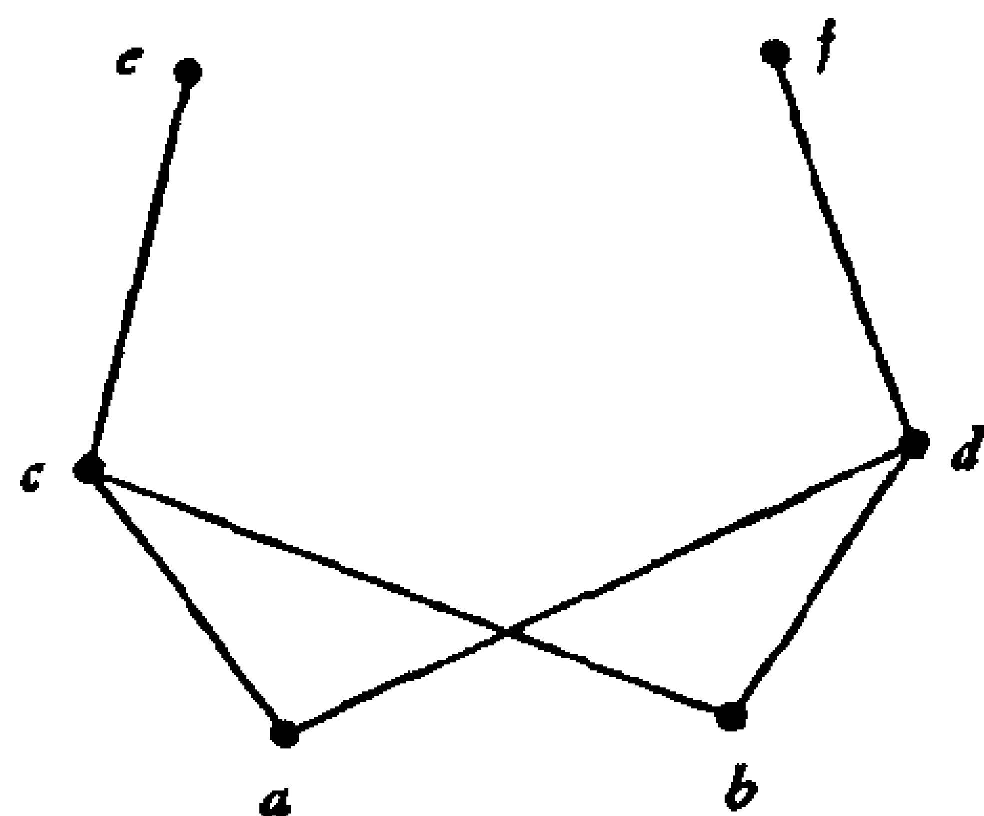


图 3 一个偏序集合

8.2. 格

定义. 格是偏序集合, 它的任意两个元素 a 和 b 都有 $l.u.b.$ 或并 $a \cup b$ 以及 $g.l.b.$ 或交 $a \cap b$.

因为 $a \cup b$ 和 $a \cap b$ 都是唯一的, 在格内并和交都是良好定义的二元运算.

定理 8.2.1. 在格内下列定律成立:

$L1$. 幂等律. $x \cap x = x$ 和 $x \cup x = x$.

$L2$. 交换律. $x \cap y = y \cap x$ 和 $x \cup y = y \cup x$.

$L3$. 结合律. $x \cap (y \cap z) = (x \cap y) \cap z$ 和 $x \cup (y \cup z) = (x \cup y) \cup z$.

$L4$. 吸收律. $x \cap (x \cup y) = x$ 和 $x \cup (x \cap y) = x$.

证明. $L1$, $L2$ 和 $L4$ 是 $l.u.b.$ 和 $g.l.b.$ 的定义的直接推论. 对于 $L3$, 令 $y \cap z = u$ 和 $x \cap u = w$. 这里 w 是 x 和 u 的下界,因而也是 x, y 和 z 的下界. 但是 x, y 和 z 的任何下界

包含在u内，所以也包含在$x\cap u=w$内．因此w是x，y和z的$g.l.b.$．同理，$(x\cap y)\cap z$也是x，y和z的$g.l.b.$，因而$x\cap(y\cap z)=(x\cap y)\cap z$．用同样的方法可以证明$x\cup(y\cup z)$和$(x\cup y)\cup z$是$x$，$y$和$z$的$l.u.b.$

定理 8.2.2. 定律$L1$，$L2$，$L3$和$L4$完全决定了格．

证明． 在满足$L1$，$L2$，$L3$和$L4$的任何体系内，$x\cap y=y$必要而且只要$x\cup y=x$．如果我们定义$x\supseteq y$在这个体系内是指$x\cap y=y$，则这体系相对于这个关系是一个偏序集合．于是从$a\cap a=a$得出$P1$．如果$a\cap b=b$和$b\cap c=c$，则$a\cap c=a\cap(b\cap c)=(a\cap b)\cap c=b\cap c=c$，这就证明了$P2$．如果$a\cap b=b$和$b\cap a=a$，由于$a\cap b=b\cap a$，我们就有$P3$．因此，在包含关系的这个定义下，已知体系是一个偏序集合．此外，$a\cap(a\cap b)=(a\cap a)\cap b=a\cap b$，$b\cap(a\cap b)=a\cap b$，因而$a\cap b$是$a$和$b$的下界．但是如果$a\supseteq x$和$b\supseteq x$，则$a\cap x=x$，$b\cap x=x$，因而$(a\cap b)\cap x=a\cap(b\cap x)=a\cap x=x$，所以$a\cap b$是$a$和$b$的$g.l.b.$．同理，如果$y\supseteq a$和$y\supseteq b$，则$a\cup y=y$和$b\cup y=y$，因而$y=(a\cup b)\cup y$；由此得出$a\cup b$不仅是$a$和$b$的上界，而且还是$l.u.b.$．

有些格还具有进一步的性质．下面是对我们有用的一些格．

定义． 如果在格L_1的元素x_i和格L_2的元素y_i之间存在一一对应$x_i\rightleftarrows y_i$，使得$x_i\cap x_j\rightleftarrows y_i\cap y_j$和$x_i\cup x_j\rightleftarrows y_i\cup y_j$，则格$L_1$和$L_2$叫做同构的．

定义． 如果格L的每个子集都有$g.l.b.$和$l.u.b.$，则L叫做完备的．

如果L的全体元素的集合具有$l.u.b.$，则它叫做全元素；又如果有$g.l.b.$，则它叫做零元素．

定义． 格L叫做分配的，假如它满足定律：

$D1.\ a\cap(b\cup c)=(a\cap b)\cup(a\cap c)$.

定义. 格 L 叫做模格，如果它满足下列模律：

M. 如果 $a\supseteq b$，则 $a\cap(b\cup c)=b\cup(a\cap c)$.

格或更一般的偏序集合说是满足极小条件的，假如任何链 $a_1\supset a_2\supset a_3\supset\cdots$ 必定是有限的；又说是满足极大条件的，假如任何链 $a_1\subset a_2\subset a_3\subset\cdots$ 必定是有限的.

定义. 在格 L 内，有限链 $x=x_0\supseteq x_1\supseteq\cdots\supseteq x_d=y$ 叫做极大的，假如 x_i 盖住 x_{i+1}，$i=0,1,\cdots,d_{-1}$；即 $x=x_0>x_1>\cdots>x_d=y$. 我们说这个链具有长度 d.

定义. 格 L 的元素 x 说是具有有限的维数 d [记做 $d(x)$]，假如 L 具有零元素 0，使得从 x 到 0 的每个链都是有限的而且 d 是从 x 到 0 的最长的极大链的长度.

8.3. 模格和半模格

在任何格内，使 $a\supseteq x\supseteq b$ 的 x 的集合组成一个子格，叫做商格 a/b. 可以表示成 $a\cup b/b$ 和 $a/a\cap b$ 的两个商格叫做彼此透视的. 又如果 a_i/b_i 与 a_{i+1}/b_{i+1} $(i=1,\cdots,n-1)$ 透视，则我们说 a_1/b_1 与 a_n/b_n 是射影的.

定理 8.3.1. 在模格内，透视的两个商格是同构的.

证明. 在模格内给了商格 $a\cup b/b$ 和 $a/a\cap b$. 对于 $a/a\cap b$ 内的任何 x，定义

$$y(x)=x\cup b.$$

对于 $a\cup b/b$ 内的任何 y，定义

$$x(y)=y\cap a.$$

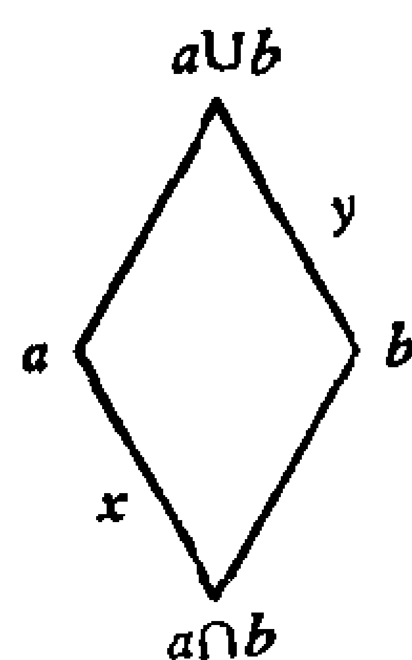


图 4 透视商格

第一个映射把 $a/a\cap b$ 的元素映成 $a\cup b/b$ 的元素，第二个映射把 $a\cup b/b$ 的元素映成 $a/a\cap b$ 的元素. 对于 $a/a\cap b$ 内的 x，$x[y(x)]=(x\cup b)\cap a$.

因为 $a\supseteq x$，我们可以应用模律，而且 $a\cap(x\cup b)=x\cup(a\cap b)=x$，因为 $x\supseteq a\cap b$．因此 $x[y(x)]=x$．同理，在 $a\cup b/b$ 内应用模律，对于 y 有 $y[x(y)]=y$．因而 $x\to y(x)$ 和 $y\to x(y)$ 导出这两个商格之间的一一对应．还要证明这个对应保持了格的运算．对于 $a/a\cap b$ 内的 x_1 和 x_2，$y(x_1\cup x_2)=(x_1\cup x_2)\cup b=(x_1\cup b)\cup(x_2\cup b)=y(x_1)\cup y(x_2)$． 再有 $x_1=x(y_1)$，$x_2=x(y_2)$，而且 $x_1\cap x_2=x(y_1)\cap x(y_2)=(y_1\cap a)\cap(y_2\cap a)=y_1\cap y_2\cap a=x(y_1\cap y_2)$． 于是 $y(x_1\cap x_2)=y[x(y_1\cap y_2)]=y_1\cap y_2=y(x_1)\cap y(x_2)$．因此两个运算在映射 $x\to y(x)$ 下都保持着． 由于对应是一一的，由此得出这两个运算在 $y\to x(y)$ 下也保持着．也可以用同样的方法证明 $y\to x(y)$ 保持这两个运算．

推论 8.3.1. 在模格内两个射影商格是同构的.

定理 8.3.2. 在模格内，如果 x 是有限维数 $d(x)$ 的元素，则从 x 到零的每个极大链有相同的长度.

证明. 证明根据对 x 的维数施行归纳法．如果 $d(x)=1$，则 $x>0$ 是从 x 到 0 的唯一的链．设 $x=x_0>x_1>\cdots>x_d=0$ 是从 x 到 0 的一个极大链，再设 $x=y_0>y_1>\cdots>y_s=0$ 是另一个极大链． 如果 $x_1=y_1$，则根据归纳假设，从 x_1 和 y_1 起的极大链有相同的长度 $d-1$，因而 $s-1=d-1$ 即 $s=d$．如果 $x_1\neq y_1$，则记 $z_2=x_1\cap y_1$． 于是商格 x/x_1 和 y_1/z_2 是透视的，而且 x/y_1 和 x_1/z_2 也是如此．因为 x/x_1 和 x/y_1 都不包含中间元素，所以 $y_1>z_2$ 和 $x_1>z_2$．因为从 x 到 0 的所有极大链的长度都是 $d-1$，所以从 z_2 到 0 的所有极大链的长度都是 $d-2$．因此从 y_1 到 z_2 到 0 的链的长度是 $d-1$，所以根据归纳假设，链 $y_1>y_2>\cdots>0$ 也是如此．因此 $x=y_0>y_1>\cdots>y_s=0$ 的长度也是 $d=s$．

作为这个定理的推论，我们得出约当-戴德金的链条件在

模格内成立.

约当-戴德金的链条件. 在两个元素之间的所有有限的极大链有相同的长度.

如果 $a \supset b$，我们可以取 b 作为商格 a/b 内的零元素然后应用定理 8.3.2..

在模格内，维数满足一个重要的关系.

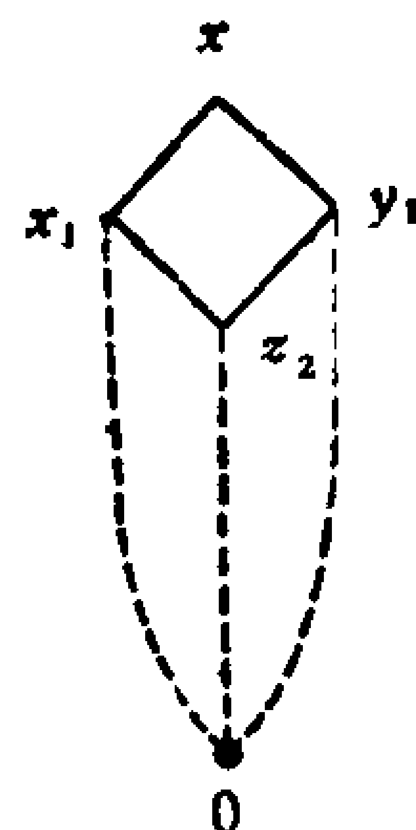


图 5 约当-戴德金条件

定理 8.3.3. 在元素的维数有限的格内，下列定律

$$d(x) + d(y) = d(x \cup y) + d(x \cap y)$$

成立，必要而且只要这个格是模格.

证明. 在模格内，商格 $x \cup y/x$ 和 $y/x \cap y$ 是同构的. 在这两个商格内的极大有限链的长度分别是 $d(x \cup y) - d(x)$ 和 $d(y) - d(x \cap y)$. 由于同构，这两个极大长度相等，因而有 (M)

$$d(x) + d(y) = d(x \cup y) + d(x \cap y).$$

反之，假定定律 (M) 在一个格内成立. 假定 $A \supseteq B$；考虑两个式子 $A \cap (B \cup C)$ 和 $B \cup (A \cap C)$. 这时

$$B \subseteq A,$$
$$B \subseteq B \cup C,$$
$$B \subseteq A \cap (B \cup C),$$
$$A \cap C \subseteq A,$$
$$A \cap C \subseteq C \subseteq B \cup C,$$
$$A \cap C \subseteq A \cap (B \cup C),$$
$$B \cup (A \cap C) \subseteq A \cap (B \cup C).$$

因此当这两个式子的维数相等时，它们是相等的. 利用等式 (M)，

$$d[B \cup (A \cap C)] = d(B) + d(A \cap C) - d(B \cap A \cap C)$$
$$= d(B) + d(A \cap C) - d(B \cap C)$$

$$= d(B\cup C) - d(C) + d(A\cap C)$$
$$= d(B\cup C) + d(A) - d(A\cup C)$$
$$= d(A) + d(B\cup C) - d(A\cup B\cup C)$$
$$= d[A\cap(B\cup C)].$$

因此 $A\cap(B\cup C) = B\cup(A\cap C)$,即模律成立.

使用盖住关系 $A > B$,我们来定义在格内可能成立的两种半模性质.

定义. 下半模性：如果当 $A > B$ 和 $A > C$, $B \neq C$ 时，就有 $B > B\cap C$ 和 $C > B\cap C$, 则格叫做下半模格.

上半模性：如果当 $A < B$ 和 $A < C$, $B \neq C$ 时，就有 $B < B\cup C$ 和 $C < B\cup C$, 则格叫做上半模格.

显然这两种半模性是彼此对偶的，而且根据定理 8.3.1, 还都是模性的推论. 我们现在来证明,在有限维的格内,这两种半模性共同导出模性.

定理 8.3.4. 在半模格 L 内,如果 $A\supseteq B$ 而且在 A 和 B 之间存在有限的极大链，则在 A 和 B 之间的所有有限极大链都有相同的长度.

证明. 这个定理的证明在主要方面与定理 8.3.2. 的相仿. 假定 L 是下半模格. 如果存在从 A 到 B 的长度为 1 的极大链，则 $A > B$, 因而从 A 到 B 没有其他的链. 我们对从 A 到 B 的极大链的长度施行归纳法. 假定

$$A = A_0 > A_1 > A_2 > \cdots > A_r = B$$

是从 A 到 B 长度为 r 的极大链，而且这个定理对长度小于 r 的链已经成立. 现在令

$$A = U_0 > U_1 > U_2 > \cdots > U_s = B$$

是从 A 到 B 的另一个极大链. 那么如果 $U_1 = A_1$,则从 $A_1 = U_1$ 到 B 的极大链根据归纳假设必定有长度 $r-1$, 因而定理成立.

其次，如果 $U_1 \neq A_1$，则根据下半模性，

$$A_1 > U_1 \cap A_1, \qquad U_1 > U_1 \cap A_1.$$

记 $U_1 \cap A_1 = V_2$. 我们将有链

$$A = A_0 > A_1 > A_2 > \cdots > A_r = B,$$
$$A = A_0 > A_1 > V_2 > \cdots > V_m = B,$$
$$A = U_0 > U_1 > V_2 > \cdots > V_m = B,$$
$$A = U_0 > U_1 > U_2 > \cdots > U_s = B.$$

对从 A_1 到 B 的链应用归纳假设，我们有 $m = r$，因而前两个链有相同的长度．第二和第三个链有相同的长度 m．再对从 U_1 到 B 的链应用归纳假设，我们有 $m = s$．因此全部四个链都有相同的长度，因而这个定理对于下半模格成立．用对偶的论证可以对上半模格证明同样的结果．

我们从这个定理知道，在半模格内，一个元素 A 的维数 $d(A)$ 是在 A 和零元素 0 之间的所有极大链的长度．在有限维的半模格内，我们有联系诸元素的维函数的不等式．

定理 8.3.5．设 L 是有限维的格．如果 L 是上半模格，则 (1) $d(X \cup Y) + d(X \cap Y) \leqslant d(X) + d(Y)$．如果 L 是下半模格，则 (2) $d(X \cup Y) + d(X \cap Y) \geqslant d(X) + d(Y)$．反之，(1) 导出上半模性．但是 (2) 并不导出下半模性．

证明．根据定理 8.3.4，如果 L 是半模格而且 $R \supset S$，则 $d(R) - d(S)$ 是在 R 和 S 之间的极大链的长度，因为从零元素到 R 的所有极大链有相同的长度，于是 R 的维数是从 R 到零包括 S 的极大链的长度．我们将在证明中利用这个事实．

假定 L 是上半模格．我们用 $A \geqslant B$ 表出 $A = B$ 或 $A > B$；把它读做"A 最多盖住 B"．那么设

$$X \cap Y = U_0 < U_1 < U_2 < \cdots < U_m = X,$$
$$X \cap Y = V_0 < V_1 < V_2 < \cdots < V_n = Y,$$

我们可以断定 $U_i \cup V_j \geqslant U_{i-1} \cup V_j$ 和 $U_i \cup V_j \geqslant U_i \cup V_{j-1}$ 对

于所有 $i=1,\cdots,m$ 和 $j=1,\cdots,n$. 我们对 $i+j$ 施行归纳法来证明这一点，$i+j$ 的最小的值是 2，而对于这个值，上半模性断定

$$U_1\cup V_1\geqslant U_1=U_1\cup V_0 \text{ 和 } U_1\cup V_1\geqslant V_1=U_0\cup V_1.$$

于是 $$U_i\cup V_j=(U_i\cup V_{j-1})\cup(U_{i-1}\cup V_j).$$

而且根据归纳假设，$U_i\cup V_{j-1}\geqslant U_{i-1}\cup V_{j-1}$ 和 $U_{i-1}\cup V_j\geqslant U_{i-1}\cup V_{j-1}$，因而根据上半模性，$U_i\cup V_j\geqslant U_i\cup V_{j-1}$ 和 $U_i\cup V_j\geqslant U_{i-1}\cup V_j$，这就是我们所要证明的. 于是对于 $j=n$，由于 $V_n=Y$，

$$Y\leqslant U_1\cup Y\leqslant U_2\cup Y\leqslant\cdots\leqslant U_m\cup Y=X\cup Y.$$

因而从 Y 到 $X\cup Y$ 的极大链的长度最多是 m. 但是我们在上面说过，这表示

$$d(X\cup Y)-d(Y)\leqslant m=d(X)-d(X\cap Y),$$

因而在上半模格内不等式 (1) 成立. 利用对偶的论证可以证明在下半模格内不等式 (2) 成立. 这就证明了定理中的正命题部分.

引理 8.3.1. 如果不等式 (1) 在 L 内成立，则从 $U>V$ 得出 $d(U)=d(V)+1$.

证明. 设 $0=U_0<U_1<U_2<\cdots<U_{t-1}<U_t=U$ 是从 0 到 U 的最长的链. 不可能存在从 0 到 U_i 的长度大于 i 的链，因为如果存在的话，我们就能构造从 0 到 U 的较长的链. 因此，$d(U)=t$ 和 $d(U_i)=i$，$i=0,\cdots,t-1$. 再有，因为 $U>V$，我们有 $d(U)\geqslant d(V)+1$，所以 $t-1\geqslant d(V)$. 让我们取 U_j 使 $U_j\subseteq V$，$U_{j+1}\nsubseteq V$. 在 $0,1,\cdots,t-1$ 中必定存在这样的 j. 于是 $U_{j+1}\cup V=U$，$U_{j+1}\cap V=U_j$. 根据不等式 (1)，$d(U_{j+1}\cup V)+d(U_{j+1}\cap V)\leqslant d(V)+d(U_{j+1})$，因而 $t+j\leqslant d(V)+j+1$ 或 $t-1\leqslant d(V)$，所以 $d(V)=t-1$，$d(U)=t=d(V)+1$.

现在我们引用引理和不等式(1)，假定 $A < B$，$A < C$ 而且 $B \neq C$. 那么 $A = B \cap C$，$d(B) = d(A) + 1$，$d(C) = d(A)+1$. 根据不等式(1)，$d(B \cup C)+d(B \cap C) \leqslant d(B)+d(C)$，这给出 $d(B \cup C) \leqslant d(A) + 2$. 但是 $B \cup C \neq B$，C，因而 $d(B \cup C) = d(B) + 1 = d(C) + 1$，给出 $B \cup C > B$，$B \cup C > C$，这说明 L 是上半模格. 因为维数 (Xd) 定义为从 0 到 X 的最长的链的长度，它并无对偶的性质，所以不能由此认为从不等式 (2) 得出 L 是下半模格. 包含五个元素 0，T，A_1，$B_1 \subset B_2$ 的格，当 $A_1 \cap B_1 = A_1 \cap B_2 = 0$，$A_1 \cup B_1 = A_1 \cup B_2 = T$ 时，满足不等式 (2) 但不是下半模格.

定理 8.3.6. 有限维的格是模格，必要而且只要它同时是上和下半模格.

证明. 我们已经看到从模性可以得出两种半模性. 而如果两种半模性成立，则根据定理 8.3.5，我们有 $d(X \cup Y) + d(X \cap Y) = d(X) + d(Y)$，因而根据定理 8.3.3. 可以得出模性.

定理 8.3.7. 有限 p 群的子群组成一个下半模格.

证明. 在 § 1.4 里定义的子群的并和交当然满足格的公理，而且一个群的子群在包含关系下是偏序的. 如果 $A > B$ 和 $A > C$，这里 A，B，C 是有限 p 群的子群，则 B 和 C 是 A 的极大子群，因而根据定理 4.3.2，它们有指数 p. 根据关于指数不等式的定理 1.5.5，$[B:B \cap C]$ 和 $[C:B \cap C]$ 最多是 p，因而是 1 或 p. 因此，如果 $B \neq C$，我们有 $B > B \cap C$ 和 $C > B \cap C$.

8.4. 主序列和合成序列

我们现在把前几节的结果联合起来，用来研究群的子群

的结构．我们考虑群G的子群的链，其中每个子群都是前面一个群的正规子群．

$$G=A_0\supseteq A_1\supseteq A_2\supseteq\cdots\supseteq A_n, \qquad (8.4.1)$$

这里每个 A_i 是 A_{i-1} 的正规子群，我们把这记做：

$$A_i\triangleleft A_{i-1}, \qquad i=1,\cdots,n. \qquad (8.4.2)$$

群 A_i 叫做群G的次不变群．

随同这个链的有商群的序列

$$A_{i-1}/A_i, \qquad i=1,\cdots,n. \qquad (8.4.3)$$

如果每个 A_i 都是G的正规子群，我们把 (8.4.1) 叫做正规链或正规序列．我们也把它叫做不变序列．如果 $A_i\triangleleft A_{i-1}$, $i=1,\cdots,n$，一般不能由此得出 $A_i\triangleleft G$，因而正规序列的要求要比 (8.4.2) 强．如果我们只假定 (8.4.2)，我们把这个序列叫做次不变序列．如果在正规序列中每个 A_i 是包含在 A_{i-1} 中的极大正规子群，则这个序列叫做主序列．如果在次不变序列中每个 A_i 是 A_{i-1} 的极大正规子群，则这个序列叫做合成序列．用格的术语来说，如果 (8.4.1) 中的包含关系是盖住关系，则正规序列叫做主序列，次不变序列叫做合成序列．此外我们可以要求群 A_i 是相对于算子集合 Ω 的容许子群．

我们可以把关于模格的一般定理解释成关于子群的定理，或者关于络上的合同关系的定理，或更一般地解释成关于任何代数体系上的合同关系（这种关系彼此可交换）的定理．使我们能得到关于群的最强结果的主要定理是定理 2.4.1．格的定理取决于模律，而这是以不同的途径在代数学内产生的．因而由于代数学中假设的变更，从格的同一个定理得出不同的定理．在群论中需要关于模性的一个辅助定理．我们说群G的子群A和B是可交换的，假如子集 AB 和 BA 是相等的．在这种情形下容易验证 $A\cup B=AB=BA$，因而子集 $AB=BA$事实上是群．根据定理 2.3.3，如果子群A和B中有一个

是正规的，则它们就是可交换的，显然它们在 $A\cup B$ 中的正规性是唯一要求的.

定理 8.4.1. 设 A, B, C 是群 G 的子群，$A\supseteq B$. 那么

$$A\cap(B\cup C)=B\cup(A\cap C)$$

成立的充分条件是 B 和 C 可交换.

证明. 像在定理 8.3.3 的证明里那样，我们总看到，如果 $A\supseteq B$，则

$$B\cup(A\cap C)\subseteq A\cap(B\cup C),$$

因而只需要证明相反的包含式. $A\cap(B\cup C)$的元素有形状 $a=bc$, $a\in A$, $b\in B$, $c\in C$，它同时是 A 和 $B\cup C$ 的元素，而且因为 B 和 C 可交换，$B\cup C$ 的元素有形状 bc. 于是 $c=b^{-1}a\in A$，因为 $B\subseteq A$. 因此这个 $c\in A\cap C$，于是 $bc\in B\cup(A\cap C)$. 因而 $A\cap(B\cup C)\subseteq B\cup(A\cap C)$，定理也就证明了. 这对于可逆络的子络也成立，在可逆络内 B 和 C 的可交换性表明 $B\cup C=BC$. $b^{-1}a=b^{-1}(bc)=c$ 的结论只要求可逆律.

定理 8.4.2. **加细定理**[1]. 设 $U=A_0\supseteq A_1\supseteq\cdots\supseteq A_n=V$ 和 $U=B_0\supseteq B_1\supseteq\cdots\supseteq B_m=V$ 是模格内从 U 到 V 的两个有限链. 那么可以用插进外加的元素 $A_{i-1}=A_{i,0}\supseteq A_{i,1}\supseteq\cdots\supseteq A_{i,m}=A_i$, $i=1,\cdots,n$ 和 $B_{j-1}=B_{j,0}\supseteq B_{j,1}\supseteq\cdots\supseteq B_{j,n}=B_j$, $j=1,\cdots,m$ 的方法来加细这两个链，使得商格 $A_{i,j-1}/A_{i,j}$ 和 $B_{j,i-1}/B_{j,i}$ 是射影的.

证明. 令 $A_{i,j}=A_i\cup(A_{i-1}\cap B_j)$, $B_{j,i}=B_j\cup(B_{j-1}\cap A_i)$, $i=1,\cdots,n$, $j=1,\cdots,m$. 于是 $A_{i,j-1}/A_{i,j}$透视于

---

1) 最初的约当-霍德尔定理为很多数学家所扩充和推广，最初的定理由约当 (C. Jordan [1]) 和霍德尔 (O. Hölder [1]) 提出. 它由耐特 (E. Noether[1]) 和克鲁勒(W. Krull [1,2]) 推广到带算子的群. 加细定理由施赖尔 (O. Schreir [4]) 和蔡森豪斯 (H. Zassenhaus [1]) 提出. 这个定理由鄂尔 (O. Ore [2]) 改写成这里给出的格论的表述. 推广到偏序集合是由鄂尔 (O. Ore [1]) 和麦克兰 (S. MacLane [3]) 做到的.

$$A_{i-1}\cap B_{j-1}/(A_{i-1}\cap B_j)\cup(A_i\cap B_{j-1}), \qquad (8.4.4)$$

因为从 $B_j\subseteq B_{j-1}$ 我们有

$$(A_{i-1}\cap B_{j-1})\cup A_i\cup(A_{i-1}\cap B_j)=A_i\cup(A_{i-1}\cap B_{j-1}). \qquad (8.4.5)$$

再有，

$$\begin{aligned}(A_{i-1}\cap B_{j-1})&\cap[A_i\cup(A_{i-1}\cap B_j)]\\ &=(A_{i-1}\cap B_j)\cup(A_{i-1}\cap B_{j-1}\cap A_i)\\ &=(A_{i-1}\cap B_j)\cup(A_i\cap B_{j-1}),\end{aligned} \qquad (8.4.6)$$

在 (8.4.6) 中用到了模律．同理，$B_{j,i-1}/B_{j,i}$ 透视于 (8.4.4) 中的商格，因而定理证明了．

这个定理和它的证明对于群 G 的次不变序列也成立，这时如果我们取 G 为带算子 Ω 的群，则子群都是容许的．这就自然地包括了不带算子的群，只要我们取 Ω 为恒同算子就成．

定理 8.4.3 (关于群的加细定理)．设 G 是带算子 Ω 的群，而且 $G=A_0\supseteq A_1\supseteq\cdots\supseteq A_n=H$ 和 $G=B_0\supseteq B_1\supseteq\cdots\supseteq B_m=H$ 是从 G 到 H 的容许子群的两个次不变序列．那么可以插进外加的容许的次不变群

$$A_{i-1}=A_{i,0}\supseteq A_{i,1}\supseteq\cdots\supseteq A_{i,m}=A_i,\quad i=1,\cdots,n \text{ 和}$$

$$B_{j-1}=B_{j,0}\supseteq B_{j,1}\supseteq\cdots\supseteq B_{j,n}=B_j,\quad j=1,\cdots,m$$

来加细这两个序列，使得商群

$$A_{i,j-1}/A_{i,j} \text{ 和 } B_{j,i-1}/B_{j,i}$$

是算子同构的．

证明．根据定理 2.4.1，容许子群的透视的 (因而射影的) 商群是算子同构的．因此，为了说明从定理 8.4.2 的证明得出这个定理，我们必须指明在证明中出现的商群 X/Y 有 $Y\lhd X$ 而且在(8.4.6)里应用的模律成立．由于容许子群的并和交仍是容许的，在证明中用到的子群都是容许的．现在 $A_{i,j}=$

$A_i \cup (A_{i-1} \cap B_j)$ 是 $A_{i,j-1} = A_i \cup (A_{i-1} \cap B_{j-1})$的正规子群，因为 A_i 和 $A_{i-1} \cap B_j$ 都被 $A_{i-1} \cap B_{j-1}$ 变到自身. 同理，$B_{j,i} \triangleleft B_{j,i-1}$. $A_{i-1} \cap B_j$ 和 $A_i \cap B_{j-1}$ 以及它们的并都是 $A_{i-1} \cap B_{j-1}$ 的正规子群，因而 (8.4.4) 是商群. 在 (8.4.6) 中，因为 A_i 在 A_{i-1} 中是正规的，A_i 与 A_{i-1} 的任何子群可交换，因而与$A_{i-1} \cap B_j$ 可交换. 因此根据定理 8.4.1，可以象在 (8.4.6) 里那样地应用模律. 于是我们的定理证明了.

在主序列或合成序列（带或不带算子的）中，不可能作进一步的加细，所以下列定理是加细定理的直接推论:

定理 8.4.4. 约当-霍德尔定理. 如果 $G = A_0 \supset A_1 \supset \cdots \supset A_n = H$ 和 $G = B_0 \supset B_1 \supset \cdots \supset B_m = H$ 是两个带算子 Ω 的主序列（或合成序列），则 $m = n$ 而且商群 A_{i-1}/A_i 算子同构于同一顺序的商群 B_{j-1}/B_j.

$m = n$ 的事实是因为在加细定理的不是单位元素群的商群之间存在一一对应.

在正规序列的情形，作为正规子群的全体子群在全体内自同构 $x \to a^{-1}xa$ 下是容许的，因而我们可以把全部内自同构包括在算子集合 Ω 内. 在全体内自同构下保持的同构叫做中心同构. 因而下列定理是加细定理的推论:

定理 8.4.5. 在正规序列的加细中，对应的商群是中心同构的.

现在如果 $x \to (x)\alpha$ 是G的中心自同构，则

$$a^{-1}(x)\alpha a = (a^{-1}xa)\alpha = (a)\alpha^{-1}(x)\alpha(a)\alpha,$$

因而 $(a)\alpha a^{-1}$ 与每个 $(x)\alpha$ 可交换，于是它必定是群的中心的元素，记做 z. 因此，对于中心自同构，$(a)\alpha = az$ 对于群的每个元素 a 和中心的一个适当的元素 z，这里 z 取决于 a. 反之，容易看出这种形式的自同构是中心自同构.

8.5. 直接分解

假定在模格内给了 m 个元素 $A_1, \cdots, A_m$，使得如果我们记 $\bar{A}_i = A_1 \cup \cdots \cup A_{i-1} \cup A_{i+1} \cup \cdots \cup A_m$，$i = 1, \cdots, m$，则 $A_i \cap \bar{A}_i = 0$（零元素），$i = 1, \cdots, m$. 于是我们说 $A = A_1 \cup \cdots \cup A_m$ 是 $A_1, \cdots, A_m$ 的直并，而且记做

$$A = A_1 \times A_2 \times \cdots \times A_m. \tag{8.5.1}$$

在群论中当 A 是 $A_1, \cdots, A_m$ 的直积时就发生这种情况.

定理 8.5.1（鄂尔定理）. 设 L 是有限维的任意模格. 如果 L 的全元素 T 有两个分解 $T = A_1 \times \cdots \times A_m$ 和 $T = B_1 \times \cdots \times B_n$，这里 A_i 和 B_j 不能再分解成直并，则 $m = n$ 而且 A_i 和 B_j 成对地是射影的.

证明. 我们来证明任何已知的 A_i（例如 A_1）可以换成与它射影的某个 B_j，使得 $T = A_1 \times A_2 \times \cdots \times A_m = B_j \times A_2 \times \cdots \times A_m$. 这是定理证明的主要部分. 在把 A_1 换成 B_j 以后，我们可以在第二个分解式中继续把 A_2 换成某个 B'_k，等等. 在代换的过程中不可能用同一个 B_j 两次，因为这就将违反任何因子与其余因子的并相交于零的要求. 我们必须有足够的 B 去代换全部的 A，而且因为每个 $B \subseteq T$，显然在全部 A 都被代换时不能有任何剩余的. 因而 $m = n$. 我们记 $\bar{A}_i = A_1 \cup \cdots \cup A_{i-1} \cup A_{i+1} \cup \cdots \cup A_m$，$i = 1, \cdots, m$ 和 $\bar{B}_j = B_1 \cup \cdots \cup B_{j-1} \cup B_{j+1} \cup \cdots \cup B_n$，$j = 1, \cdots, n$，而且对 T 的维数施行归纳法来作为证明基础，这个定理在维数为一的情形是显然的.

情形 1. 对于某个 j，$A_1 \cup \bar{B}_j = \bar{A}_1 \cup B_j = T$. 这时

$$d(A_1) = d(T) - d(\bar{B}_j) + d(A_1 \cap \bar{B}_j)$$
$$= d(B_j) + d(A_1 \cap \bar{B}_j) \geqslant d(B_j),$$

同理 $d(B_j) \geqslant d(A_1)$，这就给出 $d(A_1)=d(B_j)$. 于是 $d(A_1\cap \bar{B}_j)=d(\bar{A}_1\cap B_j)=0$，因而 $T=A_1\times \bar{B}_j=\bar{A}_1\times B_j$，所以 A_1 和 B_j 是可以相互代换的.

情形 2. 假如对于某个 j（例如 $j=1$），$A_1\cup \bar{B}_j\subset T$.

记 $D_k=A_1\cup \bar{B}_h$，$Q_h=D_h\cap B_h$，$h=1,\cdots,n$. 如果 $D_1=A_1\cup \bar{B}_1\supseteq B_1$，则 $D_1\supseteq \bar{B}_1\cup B_1=T$，与假设矛盾. 因此 $Q_1=D_1\cap B_1\subset B_1$ 而且 $d(Q_1)<d(B_1)$. T 是这些 B 的直并，因而这些 Q 的并是直并，因为 $Q_h\subseteq B_h$，$h=1,\cdots,n$.

定义

$$C=\bigcup_{h=1}^{n} Q_h.$$

于是因为 T 和 C 都是直并而且 $Q_1\subset B_1$，所以 $d(T)=d(B_1)+\cdots+d(B_n)$，

$$d(C)=d(Q_1)+\cdots+d(Q_n)<d(T). \qquad (8.5.2)$$

因为 $C\subset T$，根据关于维数的归纳假设，我们可以假定定理对于 C 成立.

我们记 $U_r=Q_1\cup\cdots\cup Q_r$. 我们希望证明 $U_r=M_r\cap N_r$，这里 $M_r=B_1\cup\cdots\cup B_r$，$N_r=D_1\cap\cdots\cap D_r$. 对于 $r=1$，这简化成 $U_1=B_1\cap D_1$，这就是 $U_1=Q_1$ 的定义. 证明根据归纳法. 我们假定 $U_j=M_j\cap N_j$. 于是 $U_{j+1}=U_j\cup Q_{j+1}=(M_j\cap N_j)\cup(B_{j+1}\cap D_{j+1})$. 这时 $D_{j+1}\supseteq \bar{B}_{j+1}\supseteq M_j\supseteq M_j\cap N_j$. 根据模律，$U_{j+1}=D_{j+1}\cap[(M_j\cap N_j)\cup B_{j+1}]$. 这时 $B_{j+1}\subseteq \bar{B}_h\subseteq D_h$，$h=2,\cdots,j$，因而 $B_{j+1}\subseteq N_j$. 最后，$U_{j+1}=D_{j+1}\cap[N_j\cap(B_{j+1}\cup M_j)]=N_{j+1}\cap M_{j+1}$，这就完成了归纳证明. 对于 $r=n$，$M_r=T$，因而

$$C=Q_1\cup\cdots\cup Q_n=D_1\cap D_2\cap\cdots\cap D_n\supseteq A_1, \qquad (8.5.3)$$

最后一个关系成立是因为 $D_h\supseteq A_1$，$h=1,\cdots,n$. 因为 $C\supseteq A_1$，我们可以运用模律得出 $(C\cap \bar{A}_1)\cup A_1=C\cap(\bar{A}_1\cup A_1)=$

$C\cap T=C$. 因为显然 $C\cap\bar{A}_1\cap A_1=0$,所以我们有

$$C=A_1\times(C\cap\bar{A}_1)=Q_1\times\cdots\times Q_n. \qquad (8.5.4)$$

因此,根据关于维数的归纳假设,定理对于 C 成立,因而 A_1 可以换成某个 Q 的某个不能分解的因子(例如 $E\subseteq Q_h$). 根据 C 中的可代换性, $d(E)=d(A_1)$. 又因为 $C=E\times(C\cap\bar{A}_1)$, 我们有 $0=E\cap C\cap\bar{A}_1=E\cap\bar{A}_1$. 因此 $d(E\cup\bar{A}_1)=d(E)+d(\bar{A}_1)=d(A)+d(\bar{A}_1)=d(T)$, 所以 $T=\bar{A}_1\cup E=E\times\bar{A}_1$. 其次, $E\subseteq Q_h=(A_1\cup\bar{B}_h)\cap B_h\subseteq B_h$ 而且 $E\cap(\bar{A}_1\cap B_h)=E\cap\bar{A}_1=0$. $E\cup(\bar{A}_1\cap B_h)=B_h\cap(E\cup\bar{A}_1)=B_h\cap T=B_h$, 因而

$$B_h=E\times(\bar{A}_1\cap B_h). \qquad (8.5.5)$$

但是根据假设, B_h 是不可分解的而且 $d(E)=d(A_1)>0$. 因此 $B_h=E$ 而且 $\bar{A}_1\cap B_h=0$. 这引出

$$T=A_1\times\bar{A}_1=B_h\times\bar{A}_1. \qquad (8.5.6)$$

又 $B_h=E\subseteq Q_h\subseteq B_h$, 因而 $B_h=Q_h=(A_1\cup\bar{B}_h)\cap B_h$. 于是 $B_h\subseteq A_1\cup\bar{B}_h$, 因而 $A_1\cup\bar{B}_h\supseteq B_h\cup\bar{B}_h=T$. 因为 $d(A_1)=d(B_h)$,我们还必须有 $d(A_1\cap\bar{B}_h)=d(A_1)+d(\bar{B}_h)-d(A_1\cup\bar{B}_h)=d(B_h)+d(\bar{B}_h)-d(T)=0$. 因此

$$T=A_1\times\bar{B}_h \qquad (8.5.7)$$

而且 A_1 和 B_h 是彼此可代换的. 这时 $h\neq 1$,因为 $A_1\cup\bar{B}_h=T$,但是 $A_1\cup\bar{B}_1\neq T$.

情形 3. 对于所有 j, $A_1\cup\bar{B}_j=T$,但是对于所有 j, $\bar{A}_1\cup B_j\subset T$, 这是不包括在情形 1 和 2 里的唯一可能情形.

交换这些 A 和这些 B 的地位, 我们可以应用情形 2 而把任何特殊的 B (例如 B_n) 换成不是 A_1 的某个 A, 经过重新编号可以取它为 A_m. 于是

$$\begin{aligned}T&=A_1\times\cdots\times A_{m-1}\times A_m\\&=B_1\times\cdots\times B_{n-1}\times A_m=\bar{B}_n\times A_m.\end{aligned} \qquad (8.5.8)$$

这时 $z\to(z\cup A_m)\cap\bar{A}_m$ 是从商格 $\bar{B}_n/0$ 到 $\bar{A}_m/0$的射影，因而根据定理 8.3.1 的推论，它是格同构．因此，如果令 $B_j^*=(B_j\cup A_m)\cap\bar{A}_m$，$j=1,\cdots,n-1$，我们从这个同构得出

$$\bar{A}_m=A_1\times\cdots\times A_{m-1}=B_1^*\times\cdots\times B_{n-1}^*.\qquad(8.5.9)$$

根据关于维数的归纳假设，定理对于 $\bar{A}_m$ 成立，因而 A_1 可以换成 $\bar{A}_m$ 中的某个 B_j^*（例如B_1^*）．这时 $B_1\cup A_m=(B_1\cup A_m)\cap(\bar{A}_m\cup A_m)=[(B_1\cup A_m)\cap\bar{A}_m]\cup A_m=B_1\cup A_m$. 因此 $B_1\cup\bar{A}_1=(B_1^*\cup A_2\cup\cdots\cup A_{m-1})\cup A_m=(A_1\cup A_2\cup\cdots\cup A_{m-1})\cup\bar{A}_m=T$，因为在 $\bar{A}_m$ 内 B_1^* 代换了 A_1. 但是这时 $A_1\cup\bar{B}_1=T=B_1\cup\bar{A}_1$，因此可以应用情形 1，因而 A_1 和 B_1 可以代换．注意情形 3 并不一定发生，而且在任何情况下，对于已知的 A_1，存在 B_j 使 A_1 和 B_j 可以代换．

对于群的这个定理是:

定理 8.5.2（魏德本-雷马克-施米特定理）[1]．设G是群，它的正规子群组成有限维的格．那么如果G能表示成两组不可分解的子群的直积 $G=A_1\times\cdots\times A_m=B_1\times\cdots\times B_n$，则 $m=n$，任何 A_i 可以换成某个 B_j，而且这些A和这些B成对地是中心同构的．这个定理对于带算子群G或对于可逆络的合同关系也都成立．

证明．因为我们已经确定正规子群组成模格，我们只需要验证直积的两种定义是协调的．在 $G=A_i\times\bar{A}_i=B_j\times\bar{B}_j$ 中我们有 A_i 和 B_j 都透视于 $G/\bar{A}_i$，因而它们是射影的．于是在 A_i 和 B_j 之间存在中心同构，而且如果认为它把 $\bar{A}_i$ 映到自身，则它就成为G的中心自同构．因此 A_i 和 B_j 的对应元素

1）这个定理最初的证明由魏德本（J. H. M. Wedderburn [1]）给出．雷马克（Remak [1,2]）改正了一个错误．施米特(O. Schmidt [Шмидт] [1]）把它推广到带算子群．格的定理（8.5.1）由鄂尔（Ore [1]）证明，但是这里给出的是经过勒霍夫（G. Birkhoff [1]）作了少许改变的形式．

只相差属于G的中心的一个因子.

8.6. 群中的合成序列

假定 $G = A_0 \supset A_1 \supset \cdots \supset A_n = H$ 是从G到子群H的合成序列. 根据定义,A_{i+1}是A_i的极大正规子群.因此A_i/A_{i+1}是单纯群,因为A_i/A_{i+1}的正规子群对应于A_i中包含A_{i+1}的正规子群(定理2.3.4). 因此如果A_i/A_{i+1}是阿贝尔群, 则它不能包含真子群, 因而必定是有限的素数阶的. 在主序列和合成序列之间存在由下列定理给出的关系:

定理 8.6.1. 设H是G的正规子群,使得存在从G到H的合成序列. 那么就存在从G到H的主序列

$$G = B_0 \supset B_1 \supset \cdots \supset B_m = H,$$

而且每个商群B_i/B_{i+1}是有限个同构的单纯群的直积.反之,如果这样的序列存在, 使得B_i/B_{i+1}是有限个同构的单纯群的直积,则就存在从G到H的合成序列.

证明. 从G到H的任何正规序列可以用插进若干项而加细成合成序列. 因此从G到H的正规序列必定短于一个合成序列, 因而它是有限长的. 于是一定存在从G到H的主序列

$$G = B_0 \supset B_1 \supset \cdots \supset B_m = H.$$

如果$m = 1$, 则G/H是单纯群,定理也就成立. 我们对m施行归纳法,因而$B_0/B_1, \cdots, B_{m-2}/B_{m-1}$中每一个都是有限个同构的单纯群的直积. 还需要证明B_{m-1}/B_m是有限个同构的单纯群的直积.

B_{m-1}/B_m的任何正规子群对应于在B_{m-1}中正规而且包含B_m的群. 因此存在极小正规子群K/B_m, 这里$K \supset B_m$而且K在B_{m-1}中是正规的. 如果$K = B_{m-1}$, 则B_{m-1}/B_m是单纯的, 因而不再需要证明什么了. 现在考虑K在G内的共轭

者 K_j. $K_j \subseteq B_{m-1}$; 因为 B_{m-1} 在 G 内是正规的. 其次,因为用 G 的元素作变形导出 B_{m-1} 的自同构,所以每个 K_i 都是 B_{m-1} 的正规子群. 再有, $\bigcup_j K_j$ 是 G 的正规子群,因为用 G 的元素作变形只不过彼此交换这些 K_j. 因此 $\bigcup_j K_j = B_{m-1}$, 因为在 B_{m-1} 和 B_m 之间没有 G 的正规子群. 取 $K = K_1$, $K_2 \nsubseteq K_1$, $K_3 \nsubseteq K_1 \cup K_2$ 和 $K_j \nsubseteq K_1 \cup \cdots \cup K_{j-1}$. $U_j = K_1 \cup \cdots \cup K_j$ 中的每一个都是 B_{m-1} 的正规子群而且包含着前一个 U_{j-1}. 因为存在从 G 到 B_m 包括 B_{m-1} 的合成序列,所以只可能存在有限个 U_j, 因而对于某个有限的 j, $B_{m-1} = K_1 \cup \cdots \cup K_j$. 现在不包含在其余的 K 的并中的 K_i 必须与其余的 K 的并相交于 B_m, 因为每个 K 都是 B_{m-1} 中包含 B_m 的极小正规子群. 因此,删去包含在其余的 K 的并中的那些 K, $B_{m-1}/B_m = K_1/B_m \cup \cdots \cup K_s/B_m$,这里每个 K_i/B_m 是 B_{m-1}/B_m 的正规子群,它与其余 K_i/B_m 的并相交于单位元素群. 但是根据定理 3.2.2, B_{m-1}/B_m 是 $K_1/B_m, \cdots, K_s/B_m$ 的直积. 现在如果 K_1/B_m 有正规真子群,则它将是 B_{m-1}/B_m 的正规子群,因为它在 K_1/B_m 内是正规的,而且其余的直接因子属于它的正规化. 但是 K_1/B_m 被假定为极小正规子群; 因此 K_1/B_m 是单纯群而且 B_{m-1}/B_m 是 s 个同构的单纯群的直积.

关于定理的逆命题,我们看出 $B_m \subset K \subset U_2 \subset U_3 \subset B_{m-1}$ 是一个合成序列的一部分,因为每个商群都是单纯的.

定理 8.6.2.[1] G 的两个次不变子群的交是 G 的次不变子群. 在合成序列中出现的两个子群的并和交都在合成序列中出现.

证明. 假定 A 和 B 是 G 的两个次不变子群. 那么根据定

1) 这些结果是属于维兰德 (H. Wielandt [2]) 的.

义我们有两个链:

$$A = A_r \lhd A_{r-1} \lhd \cdots \lhd A_1 \lhd G,$$
$$B = B_s \lhd B_{s-1} \lhd \cdots \lhd B_1 \lhd G.$$

这时在链 $A = A_r \supseteq A_r \cap B_1 \supseteq \cdots \supseteq A_r \cap B_s = A \cap B$ 中,每个子群或者等于前一个,或者是前一个的正规子群(定理2.4.1).因此

$$A \cap B \lhd C_u \lhd C_{u-1} \lhd \cdots \lhd C_1 \lhd A_r \lhd \cdots \lhd A_1 \lhd G,$$

这里 C_i 是上述链中不同的子群,而且 $A \cap B$ 是次不变的.

现在假定最初的两个链是合成序列. 那么如果 $B_1 \neq A_1$, 则 $G = A_1 \cup B_1$,因为 B_1 和 A_1 都是 G 的极大正规子群. 这时 $A_1 \cap B_1$ 是 G 的正规子群, 而且 $A_1/A_1 \cap B_1 \cong G/B_1$ 因而是单纯的;因此 $A_1 \cap B_1$ 是 A_1 的极大正规子群. 这时或者 $A_1 \cap B_1 = A_2$, 或者 $A_1 \cap B_1$ 和 A_2 都是 A_1 的极大正规子群, 因而 $A_1 = A_2 \cup (A_1 \cap B_1)$ 和 $A_2 \cap B_1 = A_2 \cap (A_1 \cap B_1)$, 所以 $A_2/A_2 \cap B_1 \cong A_1/A_1 \cap B_1 \cong G/B_1$ 是单纯的. 又 $A_1 \cap B_1/A_2 \cap B_1 \cong A_1/A_2$. 循这个途径继续下去,或者 $A = A_r = A_r \cap B_1$, 或者 $A_r \cap B_1 \lhd A_r$, 因而 $A_r/A_r \cap B_1 = G/B_1$ 是单纯的. 这时我们有合成序列

$$A_r \cap B_1 \lhd A_{r-1} \cap B_1 \lhd \cdots \lhd A_1 \cap B_1 \lhd B_1 \lhd G,$$
$$B_s \lhd B_{s-1} \lhd \cdots \lhd B_2 \lhd B_1 \lhd G,$$

这与原来的合成序列相类,但是在 B_1 之前包含较少的项. 现在用 B_2 代替 B_1 来重复上述论证,这样继续下去,最终我们就将得出从 G 到 $A \cap B$ 的合成序列.

要证明两个合成群(我们是指出现在合成序列中的子群)的并还是合成群比较困难. 我们对从 $A = A_r$ 和 $B = B_s$ 到 G 的两个合成序列的长度 r 和 s 施行归纳法. 特别可以对 $r + s$ 施行归纳法,对于 $r + s = 2$ 定理成立,因为 $A_1 \cup B_1$ 是 G 的正规子群. 为此我们需要一个引理.

引理 8.6.1. 如果C是G的合成群,它是合成群A的真子群,则存在从G到A的包括C的合成序列,特别地说,从G到C的合成序列的长度小于从G到A的合成序列的长度.

这个引理成立,是因为如果

$$C = C_t \lhd C_{t-1} \lhd \cdots \lhd C_1 \lhd G$$

和

$$A = A_r \lhd A_{r-1} \lhd \cdots \lhd A_1 \lhd G$$

是关于A和C的合成序列,则象前面一样,

$$A_r = A_r \cap C_t \lhd A_{r-1} \cap C_t \lhd \cdots \lhd A_1 \cap C_t \lhd C_t \lhd \cdots \lhd C_1 \lhd G,$$

而且从C_t到A_r的不同的群补足了从G到A_r的合成序列,后者的长度是r,因而$r > t$.

根据归纳假设,$A_{r-1} \cup B_s$和$A_r \cup B_{s-1}$都是G的合成群.如果$A_{r-1} \cup B_s$是G的真子群,则A_r和B_s是$A_{r-1} \cup B_s$内的合成群,它们作为$A_{r-1} \cup B_s$内的合成群的长度是$r' < r$和$s' < s$(根据引理).于是根据归纳假设,$A_r \cup B_s$是$A_{r-1} \cup B_s$(因而也是G)的合成群.因此可以假定$A_{r-1} \cup B_s = G$.同理我们可以在$A_r \cup B_{s-1}$是G的真子群时运用归纳法,除非也假定$A_r \cup B_{s-1} = G$.现在根据对称性假定$r < s$.于是如果$b \in B_s$,则

$$b^{-1}A_r b \lhd b^{-1}A_{r-1}b \lhd \cdots \lhd b^{-1}A_2 b \lhd A_1 \lhd G,$$

这里$b^{-1}A_1 b = A_1$,因为A_1是正规的.现在如果$b^{-1}A_r b \neq A_r$,则在A_1内A_r和$b^{-1}A_r b$都是合成群,而且这两种情形的合成序列的长度都是$r-1$.因此根据归纳假设,$A^* = A_r \cup b^{-1}A_r b$是在$A_1$内的合成群,这里从$A_1$到$A^*$的链的长度小于$r-1$.因此根据归纳假设,$B_s \cup A^*$是合成群.但是$B_s \cup A^* = B_s \cup A_r = B \cup A$.因而我们可以假定$A_r$被$B_s$的每个元素变到自身.但是$A_r$也被$A_{r-1}$的每个元素变到自身.因此$A_r$在$A_{r-1} \cup B_s = G$内是正规的.作为$G$的正规子群,我们可以取$A_r$作为$A_1$.于是$B \cup A = B_s \cup A_1 \lhd B_{s-1} \cup A_1 \lhd \cdots \lhd B_1 \cup A_1 \lhd G$.

这成立是因为 B_i 和 A_1 被 B_{i-1}变到自身，而且 A_1 作为 $B_i \cup A_1$ 的子群显然把它变到自身. 因此 $B_i \cup A_1 \triangleleft B_{i-1} \cup A_1$. 于是 $B \cup A$作为 G 中包含合成群 A 的次不变子群，本身也是合成群.

习　　题

1. 设群 G 的阶是 $p^r q^s$. 如果 G 有两个合成序列 $1 \subset A_1 \subset A_2 \subset \cdots \subset A_r \subset A_{r+1} \subset \cdots \subset A_{r+s} = G$ 和 $1 \subset B_1 \subset B_2 \subset \cdots \subset B_s \subset B_{s+1} \subset \cdots \subset B_{r+s} = G$, 这里 A_r 是 p^r 阶的而且 B_s 是 q^s 阶的，证明 G 是 A_r 和 B_s 的直积。
2. 推广习题 1 的结果，证明，如果 G 是有限群而且对于整除 G 的阶的每个素数 p, 存在 G 的合成序列，它的一项是西罗子群 $S(p)$, 则 G 是这些西罗子群的直积.
3. 证明有限个非阿贝尔的单纯群的直积的自同构互换它的各个因子.
4. 设有限生成群 G 恰好有一个极大子群 A. 证明 G 被任何不在 A 内的元素生成. 证明 G 是素数方幂阶的循环群.
5. 设有限生成群 G 恰好有两个极大子群 A 和 B 而且 $[G:A] = p$, $[G:B] = q$, 这里 p 和 q 是不同的素数. 证明 G 是 $p^i q^j$ 阶的循环群.（提示：证明 $A \cap B$ 是正规的而且 $G/A \cap B$ 是循环群.）
6. 假定 G 是有限群，$L(G)$ 是维数为 2 的. 证明，如果 G 的阶不被平方数整除，则至少有一个西罗子群是正规的. 因此得到结论：G 的阶是 p^2 或 pq, 这里 p 和 q 都是素数.

第九章 弗洛贝尼定理;可解群

9.1. 弗洛贝尼定理

定理 9.1.1. 由弗洛贝尼 (Frobenius [2]) 提出的最初形式是与群论中的许多其他结果在本质上完全不同的. 它处理的不是子群、同态或置换表示,而是有限群中的一个方程的解的个数. 它被 P. 赫尔 (Philip Hall [3]) 大大地推广了, 他同时推广了所研究的方程和关于解的知识. 但是我们在这里只给出原来定理的适当的推广.

定理 9.1.1. 设 G 是 g 阶的群而且 C 是包含 h 个共轭元素的类. 那么 c 遍历 C 时方程 $x^n = c$ 的解的个数是 (hn, g) 的倍数.

证明. 设 $A(K, n)$ 表示 G 中这种元素的子集, 它们的 n 次方幂属于子集 K, 再设 $a(K, n)$ 表示 $A(K, n)$ 中元素的个数. 对于 $g = 1$, $(hn, 1) = 1$,结论是显然的,而对于 $n = 1$, 解的个数是 $h = (h, g)$. 我们可以对 g 和 n 施行归纳法, 假定定理对于任何 $n' < n$ 和 $g' < g$ 成立.

如果 $c' = u^{-1}cu$ 而且 $x^n = c$, 则 $(u^{-1}xu)^n = c'$, 这给出在关于元素 c 的解和它的任何共轭者的解之间的一一对应. 因而 $a(C, n) = h \cdot a(c, n)$. 如果 $x^n = c$, 则 $x^{-1}cx = x^{-1}(x^n)x = x^n = c$, 因而 $x^n = c$ 的解属于 c 的正规化子 N_c, 根据定理 1.6.1 它是 g/h 阶的. 因此如果 $h > 1$,则定理在 N_c 内成立,$a(c, n)$ 是 $(n, g/h)$ 的倍数,因而 $a(C, n) = h \cdot a(c, n)$ 是 $h(n, g/h) = (hn, g)$ 的倍数,证明了定理.

现在假定 $h=1$. 如果 $n=n_1n_2$, $(n_1, n_2)=1$, $n_1>1$, $n_2>1$, 又如果 $D=A(C, n_2)$, 则 $A(C, n)=A(D, n_1)$. D 由完整的类组成. 根据归纳假设, (n_1, g) 是 $a(C, n)$ 的约数, 同理 (n_2, g) 是 $a(C, n)$ 的约数. 于是因为 (n_1, g) 和 (n_2, g) 是互素的, 所以它们的乘积 $(n_1, g)(n_2, g)=(n_1n_2, g)=(n, g)$ 整除 $a(C, n)$, 证明了定理. 现在我们可以假定 $n=p^e$ 是一个素数的 e 次方幂. 如果 p 整除 c 的阶 u, 则属于 $A(c, n)$ 的元素 x 的阶是 nu. 于是在由 x 生成的循环子群内恰好有 n 个元素属于 $A(c, n)$, 而且这些元素生成同一个子群. 因此 $a(c, n)$ 能被 n 整除.

最后我们假定 $n=p^e$ 与 c 的阶 u 互素. 因为 $h=1$, c 在 G 的中心内. G 的中心的元素中其阶不被 p 整除的组成一个阿贝尔群 B, 它的阶 b 不被 p 整除.

现在设 c_1 和 c_2 是 B 的两个元素. 因为 $p\nmid b$, 方程 $c_2=c_1y^n$ 在 B 内有唯一的解 y. 于是如果 $x^n=c_1$, 则我们有 $(xy)^n=c_2$, 因而 $a(c, n)$ 对于每个 $c\in B$ 具有同一个值. 最后, 把 G 的 g 个元素按照它们的 n 次方幂所属的类来计算, 先计算不在 B 内的那些类, 然后对 B 来计算, 这时只要用 b 乘关于其中一个元素 c 的数 $a(c, n)$, 我们得到方程

$$g=\sum_{c\in B} a(c, n)+b\cdot a(c, n).$$

现在 (n, g) 整除第一个和式中的每一项 $a(c, n)$, 这样的每一项或者适合归纳假设或者属于前面已证的情形. 再有, 因为 (n, g) 整除 g 而且与 b 互素, 所以 (n, g) 必须整除 $a(c, n)$, 这样就在所有的情形完成了定理的证明.

如果 c 是单位元素, 则 $h=1$, 就得出弗洛贝尼定理的最初形式. 这时对于所有的元素都有 $x^g=1$, 因而如果 $(n, g)=m$, 则从 $x^n=1$ 得出 $x^m=1$.

定理 9.1.2. 如果 n 是群 G 的阶的约数，则方程 $x^n=1$ 在 G 内的解的个数是 n 的倍数.

注意因为单位元素满足方程，解的个数不会是零，所以它至少是 n.

与这个定理有关的是一个有趣的猜测：如果 n 整除 G 的阶而且 $x^n=1$ 恰好有 n 个解，则这些解组成 G 的正规子群.

注意如果 G 包含 n 阶的子群 H，则 H 的元素都是解. 其次如果 $x^n=1$，则对于任意的 z，$(z^{-1}xz)^n=1$，因而 H 是正规子群. 于是问题在于证明 n 个解组成子群 H. n 整除 G 的阶这个假设是主要的，因为根据拉格朗日定理，子群的阶整除群的阶. 再有，$x^4=1$ 在三个文字的对称群（它的阶是 6）内恰好有四个解，而这些解不组成子群.

9.2. 可 解 群

群 G 的元素 $x^{-1}y^{-1}xy$ 叫做 x 和 y 的换位子，我们记

$$x^{-1}y^{-1}xy=(x,y).$$

我们还用递归规则 $(x_1,\cdots,x_{n-1},x_n)=((x_1,\cdots,x_{n-1}),x_n)$ 定义高阶的换位子. 这些是简单换位子. 更一般地，可以用逐次的交换步骤而得到的全体元素都叫做复合换位子；例如 $((a,b),(c,d,e))$. 我们递归地定义换位子的权 ω，我们说 G 的元素 g 的权是一，$\omega(g)=1$，而且令 $\omega(x,y)=\omega(x)+\omega(y)$. 因此作为换位子的元素的权取决于把它表成换位子的形式而不取决于这个元素本身.

根据换位子的定义，$(x,y)=1$ 必要而且只要 $yx=xy$. 因此，G 中的换位子都是 1，必要而且只要 G 是阿贝尔群，而且换位子可以用来衡量一个群离开阿贝尔群的程度. G 中由全体换位子 $x^{-1}y^{-1}xy$ 生成的子群 G' 叫做换位子子群或导出群.

G' 显然是 G 的完全不变子群.

定理 9.2.1. 商群 G/G' 是阿贝尔群. 如果 K 是 G 的正规子群而且 G/K 是阿贝尔群,则 $K \supseteq G'$.

证明. 在映射 $G \to G/G' = H$ 下,设 u 和 v 是 H 的任意元素而且 $x \to u$ 和 $y \to v$. 那么 $x^{-1}y^{-1}xy \to u^{-1}v^{-1}uv$. 但是 $x^{-1}y^{-1}xy \in G'$,因而 $x^{-1}y^{-1}xy \to 1 = u^{-1}v^{-1}uv$, 因此 $vu = uv$, 即 G/G' 是阿贝尔群. 现在假定 G/K 是阿贝尔群. 对于 x, $y \in G$,而且在 $G \to G/K$ 下 $x \to u$ 和 $y \to v$,我们有

$$x^{-1}y^{-1}xy \to u^{-1}v^{-1}uv = 1.$$

因而每个换位子 $x^{-1}y^{-1}xy$ 都属于 K,因此 $K \supseteq G'$.

定义. 群 G 叫做可解的, 假如序列 $G \supseteq G' \supseteq G'' \supseteq \cdots \supseteq G^{(i)} \supseteq \cdots$ 在有限步后终止于单位元素群 (例如 $G^{(e)} = 1$), 这里每个群 $G^{(i)}$ 都是前一个群的导出群.

根据定理 9.2.1, 每个商群 $G^{(i)}/G^{(i+1)}$ 都是阿贝尔群. 又如果 $G^{(i)} = G^{(i+1)}$, 则 $G^{(i)} = G^{(j)}$ 对于所有 $j \geqslant i$. 因此定理 9.2.1 中的包含式直到 $G^{(i)} = 1$ 之前都是真包含式.

定理 9.2.2. 可解群的每个子群和商群都是可解群.

证明. 设 G 是可解的而且 H 是 G 的子群. 那么根据定义 $H' \subseteq G'$, 因为 H' 由 H 中元素的全体换位子生成而 G' 由 G 中的全体换位子生成. 因此 $H'' \subseteq G''$,等等,所以如果 $G^{(e)} = 1$, 则 $H^{(e)} = 1$, 即 H 是可解的. 这时对于某个 $i < e$, $H^{(i)}$ 可以是单位元素群. 如果 $Q = G/K$ 是 G 的商群,考虑同态 $G \to Q$. 这时 Q 中的每个换位子都是 G 中的换位子的像,因此 $G' \to Q'$. 继续到 $G^{(e)} \to Q^{(e)}$, 那么当 $G^{(e)} = 1$ 时有 $Q^{(e)} = 1$. 对于某个 $i < e$, $Q^{(i)}$ 也可以是单位元素群.

定理 9.2.3[1]. 有限阶的群是可解的, 必要而且只要从 G

1) 合成序列的这个性质在历史上是可解性的最初定义, 但是这个定义不能用到无限群. 伽罗瓦理论指出: 多项式方程 $f(x) = 0$ 可以用根式解,必要而且只要它的伽罗瓦群可解.

到1的合成序列中的商群都是素数阶的循环群.

证明. 假定 $G = A_0 \supset A_1 \supset \cdots \supset A_r = 1$,这里每个 $A_{i-1}/A_i\ (i = 1, \cdots, r)$ 都是素数阶的循环群. 根据定理 9.2.1,因为 G/A_1 是阿贝尔群, $A_1 \supseteq G'$. 同理 $A_2 \supseteq A_1' \supseteq G''$,最后 $A_r \supseteq G^{(r)}$,因而 $G^{(r)} = 1$,所以 G 是可解的. 反之,假定 G 是可解的和有限的. 因为 G/G' 是阿贝尔群,在

$$G \supset G' \supset G'' \supset \cdots \supset G^{(c)} = 1$$

中存在极大正规子群 $A_1 \supseteq G'$. 因为 G/A_1 是单纯的和阿贝尔的,所以它是素数阶的循环群. 同理,因为 A_1 是可解的,所以 A_1 包含极大正规子群 A_2,使得 A_1/A_2 是素数阶的循环群. 这样继续下去, 最后有 $G = A_0 \supset A_1 \supset \cdots \supset A_r = 1$, 其中每个 A_{i-1}/A_i 是素数阶的循环群. 根据若当-霍德尔定理, 对于每个合成序列都有同样的结果.

定理 9.2.4. 在有限可解群 G 的主序列

$$G = C_0 \supset C_1 \supset \cdots \supset C_s = 1$$

中,商群 $C_{i-1}/C_i\ (i = 1, \cdots, s)$ 是初等阿贝尔群.

证明. 根据定理 8.6.1, C_{i-1}/C_i 是同构的单纯群的直接乘积. 根据定理 9.2.2.,这些单纯群是可解的因而是素数阶的循环群. 因此 C_{i-1}/C_i 是同一个素数 p 阶的若干个循环群的直积, 因而它是初等阿贝尔群. 反之, 如果 G 有这样的主序列,则因为商群是阿贝尔群,所以 G 是可解的. 设 $C_0/C_1, \cdots, C_{s-1}/C_s$ 的阶分别是 $c_1, \cdots, c_s$,这些数叫做 G 的主因子,已经指出过它们是素数的方幂. 商群 G/K 的主因子显然是 G 的主因子的子集, 因为存在 G 的包括正规子群 K 的主序列. 对于 G 的子群 H,序列

$$H \supseteq H \cap C_1 \supseteq H \cap C_2 \supseteq \cdots \supseteq H \cap C_s = 1$$

中不相同的项组成 H 中的正规序列, 因而它本身或它的加细是 H 的主序列, 于是 H 的主因子是 G 的主因子的约数, 因为

$H\cap C_{i-1}/H\cap C_i$ 同构于 C_{i-1}/C_i 的商群.

定理 9.2.5. 群 G 的下列两个性质等价于可解性:

1) G 具有有限的正规序列

$$G=A_0\supseteq A_1\supseteq A_2\supseteq\cdots\supseteq A_s=1,$$

其中每个 $A_{i-1}/A_i\ (i=1,\cdots,s)$ 都是阿贝尔群.

2) G 具有有限的次不变序列

$$G=B_0\supseteq B_1\supseteq B_2\supseteq\cdots\supseteq B_t=1,$$

其中每个 $B_{i-1}/B_i\ (i=1,\cdots,t)$ 都是阿贝尔群.

证明. 如果 G 是可解的,则它的导出序列

$$G\supset G'\supset G''\supset\cdots\supset G^{(r)}=1$$

是有限的正规序列,其中 $G^{(i-1)}/G^{(i)}\ (i=1,\cdots,r)$ 是阿贝尔群,因而性质 (1) 成立,当然性质 (2) 也成立. 还需要证明从性质 (2) 得出可解性. 这时如果 $G=B_0\supseteq B_1\supseteq B_2\supseteq\cdots\supseteq B_t=1$ 是次不变序列,其中 $B_{i-1}/B_i\ (i=1,\cdots,t)$ 是阿贝尔群;则由于 $G/B_1=B_0/B_1$ 是阿贝尔群, $B_1\supseteq G'$. 同理, 如果 $B_{i-1}\supseteq G^{(i-1)}$, 则 $B_i\supseteq B'_{i-1}\supseteq G^{(i)}$. 因此最终地有 $1=B_t\supseteq G^{(t)}$ 和 $G^{(t)}=1$,因而 G 是可解的.

推论 9.2.1. 如果群 G 具有正规子群 H 使得 H 和 G/H 都是可解的,则 G 是可解的.

如果 $G/H\supseteq A_1/H\supseteq\cdots\supseteq A_{r-1}/H\supseteq H/H$ 和 $H\supseteq B_1\supseteq\cdots\supseteq B_{s-1}\supseteq 1$ 分别是 G/H 和 H 中满足第二个性质的序列,则 $G\supseteq A_1\supseteq\cdots\supseteq A_{r-1}\supseteq H\supseteq B_1\supseteq\cdots\supseteq B_{s-1}\supseteq 1$ 是 G 中满足第二个性质的序列.

9.3. 关于可解群的推广的西罗定理

有限群的西罗子群具有这样的性质,它的阶 $m=p^a$ 与它的指数 n 互素. P. 赫尔 (Philip Hall [1]) 证明了推广到可解

群的以子群表出的西罗定理，这些子群的阶 m 与它们的指数 n 互素，但是并不要求 m 是素数的方幂.

定理 9.3.1. 设 G 是 mn 阶的可解群，这里 $(m, n)=1$. 那么

1) G 具有至少一个 m 阶的子群.

2) 任何两个 m 阶子群是共轭的.

3) 阶 m' 整除 m 的任何子群包含在一个 m 阶子群内.

4) m 阶子群的个数 h_m 可以分解因子，使得每个因子 (a) 取 m 的某个素因子为模而与 1 同余，和 (b) 是素数的方幂而且整除 G 的一个主因子.

证明. 注意当 $m=p^a$ 是素数的方幂时，性质 (1) 和 (3) 在第一个西罗定理（定理 4.2.1）里给出，性质 (2) 是第二个西罗定理，而性质 (4) 是第三个西罗定理的更强的表述.

证明根据对 G 的阶施行归纳法. 当 G 的阶是素数的方幂时定理显然成立. 证明主要利用定理 9.2.4 里所给的 G 的主序列的结构和商群的结构（定理 2.3.4）.

情形 1. G 具有正规真子群 H，它的阶是 m_1n_1，指数是 m_2n_2，这里 $m=m_1m_2$, $n=n_1n_2$ 而且 $n_1<n$.

关于性质 (1)，G/H 根据归纳假设包含 m_2 阶的子群，它对应于 G 的 mn_1 阶子群 D. 根据归纳假设 D 包含 m 阶子群.

关于性质 (2)，如果 M 和 M' 是 m 阶的两个子群，则 $M\cup H=MH$ 和 $M'\cup H=M'H$ 是其阶整除 $m_1m_2\cdot m_1n_1$ 的子群，因为 $M\cup H/H\cong M/M\cap H$（定理 2.4.1）. 因为这阶也整除 mn，所以它必定整除 mn_1. 但是它还是 m 的倍数和 n_1 的倍数. 因此 $M\cup H$ 和 $M'\cup H$ 的阶都是 $mn_1=m_1n_1m_2$，因而 $M\cup H/H$ 和 $M'\cup H/H$ 都是 G/H 的 m_2 阶子群，根据归纳假设它们是共轭的. 如果 G/H 中的 a^* 把 $M'\cup H/H$ 变成 $M\cup H/H$，而且 G 中的 a 在同态 $G\to G/H$ 下映到 a^*，则 $a^{-1}(M'\cup H)a$ 映

到 $M\cup H/H$;换句话说,$a^{-1}(M'\cup H)a=M\cup H$. 这时 $a^{-1}M'a$ 和M在 $M\cup H$ 内的阶是 m, 因而根据归纳假设是共轭的.因此M和 M' 在G内是共轭的.

关于性质 (3),如果 M_1 是 m' 阶的子群, m' 是m的约数, 则 $M_1\cup H/H$ 的阶是 m_2 的约数, 因而它属于 G/H 的 m_2 阶子群. 因此 M_1 属于G的对应的 mn_1 阶子群, 于是根据关于这个群的归纳假设,M_1 属于一个m阶的子群.

关于性质 (4), 根据 (2) 的证明,m阶子群M的共轭者的个数 h_m 是 G/H 中的 m_2 阶子群的个数 h_{m_2} 和M在 $M\cup H=D$ 中的共轭者的个数的乘积. 这时D的主因子整除G的主因子而且 G/H 的主因子是G的主因子的子集. 因此根据归纳假设, h_m 是满足条件 (4) 的两个因子的乘积, 因而这个性质证明了.

现在设在主序列内的最小正规子群K的阶是 p^a, 这里 p 是素数. K满足情形 1 中关于H的要求, 除掉 $n=p^a$. 因而我们可以假定每个极小正规子群的阶是p^a. 但是作为 p^a阶的西罗子群,只可能存在一个这种正规子群.

情形 2. G包含阶为 $n=p^a$ 的唯一的极小正规子群 K.

关于性质 (1), 设L是真包含着K的极小正规子群. 那么 L/K 的阶是 q^b,这里 $q\neq p$. 设Q是L的 q^b 阶西罗子群, 而且M是Q在G内的正规化子. 考虑 $M\cap K=T$. T 是M的正规子群,而且作为K的子群,它是初等阿贝尔群. T 的每个元素与Q的每个元素可交换, 因为Q的一个元素和T的一个元素的换位子属于 $T\cap Q=1$. 因此T属于L的中心 C,后者作为L的特征子群是G的正规子群. 因为K是极小的和唯一的, $C=K$或 $C=1$. 如果 $C=K$, 则 $L=K\times Q$, 而且Q是G的正规子群, 这与K的唯一性矛盾. 因此 $T=C=1$. 于是Q是它自己在L内的正规化子而且Q在L内的共轭者的

个数等于它在L内的指数；这是说Q在L内有$n=p^a$个共轭者．Q在G内的共轭者属于L，因为L是正规的．因此Q在G内有$n=p^a$个共轭者，因而M在G内的指数是$n=p^a$，即它是m阶的．

关于性质(2)和(4)，Q的p^a个共轭者的正规化子是共轭的和互不相同的．因而我们有p^a个共轭的m阶子群．又L内q^b阶西罗子群的个数$p^a\equiv 1\ (\bmod q)$．现在如果M'是m阶的任何子群，则$M'\cup L$的阶能被m和n整除，因而$M'\cup L=G$．因为$G/L=M'/M'\cap L$,我们看到$M'\cap L$是q^b阶的,因而是Q的共轭者,又$M'\cap L$在M'内是正规的,因而M'是Q的共轭者的正规化子．于是这p^a个m阶的共轭子群已经是全部m阶子群．这就证明了(2)和(4)．

关于性质(3)，设M'是m'/m阶的子群．那么如果M是m阶的,则$M\cap(M'\cup K)=M^*$是m'阶的,而且根据关于$M'\cup K$的性质(2),M^*共轭于M'．因此M'包含在M的一个共轭者内,这就证明了(3)．

可解群的上述性质在单纯群内常常不成立．60阶的单纯群（五个文字的交替群）没有15阶的子群因而违反了(1);它包含着由(123)和(12)(45)生成的6阶子群，这子群不包含在12阶的子群内,因而违反了(3)．最后，5阶的西罗子群的个数是六,而因为$6=2\cdot 3$,所以性质(4)也不成立．8阶的初等阿贝尔群A的自同构群是168阶的单纯群G．G传递地交换A的七个2阶子群，也传递地交换七个4阶子群．因此G具有指数为7和阶为24的子群的两个不同的共轭类,因而违反了性质(2)．

定理9.3.1的第一个性质实际上判定了可解群.为了证明这一点我们需要一个定理，它将在第16章里作为定理16.8.7而证明．

定理 9.3.2 (伯恩赛德). p 和 q 都是素数的 $p^a q^b$ 阶群是可解的.

假定这个定理成立，我们就可以用第一个性质来判定可解群. 在 g 阶群 G 内, p 补群是指这样的子群 S'_p, 它的指数 p^e 是整除 G 的阶 g 的 p 的最高方幂. 因而第一个性质断定可解群内 p 补群的存在. 我们利用伯恩赛德定理来证明它的逆.

定理 9.3.3. 如果群 G 对于整除它的阶的每个素数 p 都包含一个 p 补群, 则 G 是可解的.

证明. 设 G 的阶是 g 而且 $g = p_1^{e_1}\cdots p_r^{e_r}$, 这里 p_i 都是素数. 如果 H_1 和 H_2 是指数分别为 $p_i^{e_i}$ 和 $p_j^{e_j}$ 的子群, 则因为指数是互素的, 所以 (定理 1.5.6) $H_{12} = H_1 \cap H_2$ 的指数是 $p_i^{e_i} p_j^{e_j}$. 再根据定理 1.5.6, H_{12} 与 p_k 补群的交的指数是 $p_i^{e_i} p_j^{e_j} p_k^{e_k}$. 继续这个步骤, 当 $g = mn$ 而且 $(m, n) = 1$ 时, 我们可以找出阶为 m 而且指数为 n 的子群, 它是整除 n 的素数 p 的 p 补群的交. 于是 p 补群的存在就足以证明阶 m 与指数 n 互素的子群的存在, 也足以证明整个第一个性质.

我们假定定理对于其阶小于 g 的群成立, 然后施行归纳法. 在 p^a 阶群内, 指数 p 的每个极大子群是正规子群 (推论 4.2.2), 因而 p^a 阶群是可解的. 假定伯恩赛德定理成立, 即 $p^a q^b$ 阶群是可解的, 因而我们只要考虑 G 的阶至少能被三个不同的素数整除的情形. G 包含子群 H, 它的阶 $p^a q^b = m$ 与它的指数 n 互素, $mn = g$, 这里 p 和 q 是整除 g 的两个不同的素数. 于是 H 作为可解群, 至少包含正规子群 K, 它是阶为素数方幂 p^i 的初等阿贝尔群 (定理 9.2.4). 然而 K 包含在 p^a 阶西罗子群 $P \subseteq H \subseteq G$ 内. 这时在 G 内的 q 补群 L^* 就包含西罗子群 p^*, 它在 G 内共轭于 P. 因此经过 G 的某个元素的变形, 可以把 L^* 变成包含 P 的 q 补群 L, 这时 $L \supseteq P$ 和 $H \supseteq P$, 因而根据它们的阶有 $L \cap H = P$, $L \cup H = G$, 而且事实上有

$LH=G$，因为 LH 包含 g 个不同的元素．于是 L 的每个傍系包含 H 的一个元素，因此 L 的全体共轭者可以由元素 $h\in H$ 的变形得出．但是因为 K 在 H 内是正规的，$h^{-1}Kh=K$，所以 $h^{-1}Lh\supseteq K$．因而 L 的共轭者的交 M 是 G 的真子群，因为 $K\subseteq M\subset L$，而且 M 作为整个一类共轭者的交集是 G 的正规子群．

因此 G 包含正规真子群 M．如果 S'_p 是 G 内的 p 补群，则 $S'_p\cap M$ 是 M 内的 p 补群而且 $S'_p\cup M/M$ 是 G/M 内的 p 补群．因而 M 和 G/M 都具有 p 补群，根据归纳假设，它们是可解的．所以 G 是可解的．

9.4. 关于可解群的进一步的结果

定理 9.4.1. 如果 G 是 g 阶的可解群，而且 n 是 g 的约数，使得 $x^n=1$ 恰好有 n 个解，则这些解组成 G 的正规子群．

证明．当 g 是素数时定理成立，我们假定定理对于阶数比 G 低的可解群成立．现在 G 作为可解群包含一个最小正规子群 K，它是 p^i 阶的初等阿贝尔群．我们考虑两种情形，一种情形 p 整除 n，另一种情形 p 不整除 n．

情形 1. p 整除 n．

这时 K 的每个元素是 p 阶的，因而都是 $x^n=1$ 的解．设 $n=p^jn_1$，$g=p^sg_1$．于是 G/K 的阶是 $p^{s-i}g_1$，而且这个阶当 $j\geqslant i$ 时被 $u=p^{j-i}n_1$ 整除，当 $j<i$ 时被 $u=n_1$ 整除．因此在 G/K 内有 ku 个元素 z 使 $z^u=1$．现在如果 x 是 G 的元素使得在同态 $G\to G/K$ 下 $x\to z$ 而且 $z^u=1$，则 $x^u\in K$，因而 $x^{up}=1$，于是因为 up 整除 n，所以对于这样的 x 有 $x^n=1$．然而这些 x 是 K 在 G/K 内的 ku 个傍系的元素．因此在 G 内至少有 kup^i 个 x 满足 $x^n=1$．现在如果 $j<i$，则 up^i 是 n 的真倍数，就产生 $x^n=1$ 的多于 n 个解而与假设矛盾．因此

$j \geqslant i$ 而且 $up^i = n$,因而至少有 kn 个解. 于是 $k = 1$ 而且在 G/K 内 $z^u = 1$ 恰好有 u 个解. 根据归纳假设, 这 u 个解组成 G/K 的正规子群 H/K, 于是在 G 中的对应群 H 是 G 的 $up^i = n$ 阶正规子群,它的元素是 $x^n = 1$的 n 个解.

情形 2. p 不整除 n.

这时 n 整除 G/K 的阶, 因而在 G/K 内 $z^n = 1$ 有 kn 个解. 于是如果 $y \in G$ 而且在同态下 $y \to z$,则 $y^n \in K$ 而且 $y^{pn} = 1$. 因此在 G 内 K 有 kn 个傍系包含元素 y 满足 $y^{pn} = 1$. 我们来断定每个傍系 Ky 产生 $x^n = 1$ 的一个不同的解. 因为设 Ky_1 和 Ky_2 是 K 的不同的傍系而且 $y_1 \to z_1$, $y_2 \to z_2$, $z_1 \neq z_2$. 于是 $y_1^{pn} = 1$, $y_2^{pn} = 1$, 因而 $y_1^p = x_1$ 和 $y_2^p = x_2$ 是 $x^n = 1$ 在 G 内的解. 如果 $y_1^p = y_2^p$,则 $z_1^p = z_2^p$. 然而 $z_1^n = 1$, $z_2^n = 1$, 而且因为 $(p, n) = 1$, 由此我们就有 $z_1 = z_2$ 而与假设矛盾. 因此如果 $z^n = 1$ 在 G/K 内有 kn 个解,则 $x^n = 1$ 在 G 内至少有 kn 个解. 因而 $k = 1$,而且根据归纳假设, G/K 包含 n 阶正规子群 U/K. 于是 G 内的对应群 U 是 $p^i n$ 阶的. 但是 U 作为可解群包含 n 阶的 p 补群 H. 因而 H 的 n 个元素是 $x^n = 1$ 的 n 个解, 而且因为用 G 的任何元素作变形, 都使 $x^n = 1$ 的解彼此交换,所以 H 是 G 的正规子群.

定理 9.4.2. 如果群 G 的导出群 $G' \supset G'' \supset G''' \supset \cdots$ 的两个相继的商群都是循环群,则后一个商群是单位元素群.

证明. 设 G'/G'' 和 G''/G''' 是循环群,我们可以取 $G''' = 1$ 来证明 $G'' = 1$. 设 b 是 G'' 的生成元素. 现在 G 是 G'' 的正规化子,而且如果 Z_b 是 G'' 的中心化子,则 G/Z_b 同构于一个循环群的自同构群,因而是阿贝尔群. 因此 $Z_b \supseteq G'$. 于是 G'' 在 G' 的中心内, 而且 G' 从添加单独一个元素到 G'' 而得出. 于是 G' 是阿贝尔群,因而 $G'' = 1$,这就是所要证明的.

如果 G/G' 和 G' 都是循环群, 则我们说 G 是亚循环群.

这时 $G''=1$，我们有的是两步亚循环群. 根据定理 9.4.2，不可能存在三步亚循环群.

定理 9.4.3. 如果 g 阶有限群 G 的西罗子群都是循环群，则 G 是亚循环群而且由满足下列定义关系的两个元素 a 和 b 生成：

$$a^m=1,\quad b^n=1,\quad b^{-1}ab=a^r,$$

$$mn=g,\quad (r-1,nm)=1,\quad r^n\equiv 1(\bmod m).$$

反之，由这样的定义关系给出的群的全体西罗子群都是循环群.

证明. 我们必须先证明 G 是可解的. 设 $g=p_1^{e_1}\cdots p_s^{e_s}$，$p_1<p_2<\cdots<p_s$，是 g 的素因子分解. 我们先证明对于 $m=p_j^{f_j}p_{j+1}^{e_{j+1}}\cdots p_s^{e_s}$，$f_j\leqslant e_j$，方程 $x^m=1$ 恰好有 m 个解. 这在 $m=g$ 时当然成立. 因此只要证明，如果 $x^{mp}=1$ 恰好有 mp 个解而且 p 是整除 mp 的最小素数，则 $x^m=1$ 恰好有 m 个解. 因为属于 p 的西罗子群是循环群，所以如果 p^{f+1} 是整除 pm 的 p 的最高方幂，则在 G 内存在 p^{f+1} 阶的元素；因此 $x^{mp}=1$ 的解并不都是 $x^m=1$ 的解. 这说明 $x^m=1$ 的 km 个解（定理 9.1.2）是 $x^{mp}=1$ 的解的真部分，因而 $1\leqslant k<p$. 满足 $x^{mp}=1$ 而不满足 $x^m=1$ 的元素的阶 t 恰好被 p^{f+1} 整除. 于是就有生成同一个循环群的 $\varphi(t)$ 个元素，它们的阶都恰好被 p^{f+1} 整除，这时因为 p^{f+1} 整除 t，$\varphi(t)$ 能被 $p-1$ 整除. 因此，满足 $x^{pm}=1$ 而不满足 $x^m=1$ 的元素的个数 $pm-km=(p-k)m$ 能被 $p-1$ 整除. 因为 p 是整除 mp 的最小素数，所以 $p-1$ 与 m 没有公因子. 因而 $p-1$ 整除 $p-k$，而因为 $1\leqslant k<p$，这只有在 $k=1$ 时才能成立；也就是在 $x^m=1$ 恰好有 m 个解时才成立. 特别对于 $m=p_s^{e_s}$，$x^m=1$ 恰好有 m 个解. 但是存在这个阶的西罗子群，因而它必定是 G 的正规子群. 这是循环群当然也是可解群.

我们曾证明具有循环的西罗子群的群 G 必定有正规子群 H. 于是 H 和 G/H 也都有循环的西罗子群. 我们可以归纳地假定 H 和 G/H 可解，因而 G 也可解，因为素数阶的群是可解的.

西罗子群是循环群的阿贝尔群本身也是循环群. 因此在 $G\supset G'\supset G''\supset\cdots$ 中商群是循环群，因而根据定理 9.4.2，$G''=1$. 如果 $G'=1$，则 G 是循环群，而当我们取 $b=1$，$r=1$，$n=1$，$m=g$ 时就得到这个情形. 因此，假定 $G'\neq 1$，而且设 a 是 G' 的生成元素，$a^m=1$. 设 b 是傍系 $G'b$ 的元素，$G'b$ 是循环的商群 G/G' 的生成元素. 于是 a 和 b 生成 G 而且 $b^{-1}ab=a^r$，$r\neq 1$，因为 G' 是正规子群；如果 $r=1$，则 G 将是阿贝尔群，因而是循环群，这与假设矛盾. 如果 G/G' 的阶是 n，则 $b^{-n}ab^n=a^{r^n}=a$ 而且 $r^n\equiv 1\ (\mathrm{mod}\,m)$. 现在 G 的每个元素有形状 b^ja^i，因而最一般的换位子 (b^ua^v, b^ja^i) 可以由形状 (a^k, b^t) 的换位子表出；后面这些是 $a^{-1}b^{-1}ab=a^{r-1}$ 的方幂. 因此 a^{r-1} 生成 G'，所以 $(r-1, m)=1$. 现在 $b^n\in G'$ 是 a 的方幂 a^j，它与 b 可交换，因而 $a^{rj}=a^j$，但是因为 $(r-1, m)=1$，$j=0$，所以 $b^n=1$. 如果 m 和 n 有公共的素因子 p，则 $a^{m/p}$ 和 $b^{n/p}$ 将生成 p^2 阶的非循环子群，矛盾于西罗子群是循环群的事实. 因此 $(m,n)=1$. 这证明了定理的正命题.

反之，设 m，n，r 和 g 满足上述关系. 那么因为 $r^n\equiv 1(\mathrm{mod}\,m)$，所以 $a\to a^r$ 是由 a 生成的循环群的自同构，a 的 n 次方幂（也可能是较低的方幂）是单位元素. 因而对于 mn 个元素 b^ja^i（j 取模 n，i 取模 m）和乘积法则 $b^ja^i\cdot b^ka^t=b^{j+k}a^h$ $(h=ir_k+t)$，我们可以验证结合律和逆的存在，因而得出具有关系 $a^m=1$，$b^n=1$，$b^{-1}ab=a^r$ 的阶为 $g=mn$ 的群，而且发现乘积法则是这些定义关系的推论. 在这个群内，每个换位子是 $a^{-1}b^{-1}ab=a^{r-1}$ 的方幂，于是因为 $(r-1,m)=1$，

G' 由 a 生成．因为 $(m,n)=1$，每个西罗子群都是子群 $\{a\}$ 或 $\{b\}$ 的共轭者，因而是循环群.

推论 9.4.1. 如果群 G 的阶不含平方因子，则 G 是定理 9.4.3 中那种类型的亚循环群.

这是因为西罗子群都是素数阶的因而都是循环群.

习　　题

1．证明，如果有限群 G 的阶能被 12 整除而且 $x^{12}=1$ 在 G 内恰恰有 12 个解，则这些解组成一个正规子群.
2．证明，如果 G 的阶是 p^2q，这里 p 和 q 是不同的素数，则 G 有一个西罗子群是正规的而且 G 是可解的.
3．证明，如果 G 的阶是 p^2qr，这里 p，q，r 是不同的素数，则或者 G 是可解的，或者 G 是 60 阶的交替群 A_5.（提示：利用定理 14.3.1 和它的推论．）
4．证明，如果 $x^n=1$ 在群 G 内恰好有 m 个解 $x_1=1$，x_2，$\cdots$，x_m，则 $K=\{x_1,\cdots,x_m\}$ 是 G 的正规子群，它的元素有形状 $x_2^{a_2}x_3^{a_3}\cdots x_m^{a_m}$ 而且 K 的阶最多是 $(m-1)^n$.

第十章 超可解群和幂零群

10.1. 定 义

有两种就质上说比可解性更强的群的性质值得讨论一下. 这两种性质就是超可解性和幂零性.

定义. 如果群 G 具有有限的正规序列 $G=A_0\supseteq A_1\supseteq A_2\supseteq\cdots\supseteq A_r=1$, 其中每个商群 A_{i-1}/A_i 都是循环群, 则 G 叫做超可解的.

定义. 如果群 G 具有有限的正规序列 $G=A_0\supseteq A_1\supseteq A_2\supseteq\cdots\supseteq A_r=1$, 其中商群 A_{i-1}/A_i 包含在 G/A_i 的中心内, $i=1,\cdots,r$, 则 G 叫做幂零的.

因为在这两种情形里, A_{i-1}/A_i 都是阿贝尔群, 所以这两个性质导出 G 的可解性. 注意在超可解群 G 内, $A_{i-1}=\{b_{i-1}, A_i\}$, 这里 b_{i-1} 是 A_{i-1} 的映成循环群 A_{i-1}/A_i 的生成元素的任意元素, 因而 G 是有限生成的. 因为幂零群包括全部阿贝尔群, 所以显然幂零群不一定是有限生成的.

白尔 (Baer [12]) 以更广的方式定义超可解性, 说 G 是超可解的, 假如 G 的每个同态像包含循环的正规子群. 他证明对于有限生成群, 这定义等价于我们的定义, 但是在这个较广的定义下, 本章中证明的性质并不成立.

10.2. 下和上中心序列

我们把换位子 $x^{-1}y^{-1}xy$ 记做 (x, y). 对于子群 A 和 B,

用 (A, B) 表示由 $a \in A$ 和 $b \in B$ 的全体 (a, b) 生成的群. 我们用下列规则定义简单换位子

$$(x_1, \cdots, x_{n-1}, x_n) = ((x_1, \cdots, x_{n-1}), x_n),$$

同理对于子群 $A_1, \cdots, A_{n-1}, A_n$, 我们定义

$$(A_1, \cdots, A_{n-1}, A_n) = ((A_1, \cdots, A_{n-1}), A_n).$$

让我们把共轭记做方幂,令

$$a^x = x^{-1}ax.$$

关于高阶换位子有一系列重要的恒等式:

$$(y, x) = (x, y)^{-1}. \qquad (10.2.1.1)$$

$$(xy, z) = (x, z)^y (y, z) = (x, z)(x, z, y)(y, z). \qquad (10.2.1.2)$$

$$(x, yz) = (x, z)(x, y)^z = (x, z)(x, y)(x, y, z). \qquad (10.2.1.3)$$

$$(x, y^{-1}, z)^y (y, z^{-1}, x)^z (z, x^{-1}, y)^x = 1. \qquad (10.2.1.4)$$

$$(x, y, z)(y, z, x)(z, x, y) = (y, x)(z, x)(z, y)^x \cdot$$
$$\cdot (x, y)(x, z)^y (y, z)^x (x, z)(z, x)^y. \qquad (10.2.1.5)$$

这些恒等式可以从换位子的定义通过直接计算来验证.

我们按下列规则定义群 G 的子群序列:

$$\Gamma_1(G) = G,$$
$$\Gamma_k(G) = \{(x_1, \cdots, x_k)\},$$

这里 $x_i \in G$ 是任意取的.

因为 $(y_1, y_2, \cdots, y_{k+1}) = [(y_1, y_2), y_3, \cdots, y_{k+1}]$, 所以对于所有的 k 有 $\Gamma_{k+1}(G) \subseteq \Gamma_k(G)$. $\Gamma_k(G)$ 显然是 G 的完全不变子群. 序列

$$G = \Gamma_1(G) \supseteq \Gamma_2(G) \supseteq \Gamma_3(G) \supseteq \cdots$$

叫做 G 的下中心序列.

定理 10.2.1. $\Gamma_{k+1}(G) = (\Gamma_k(G), G)$.

证明. 因为 $(y_1, \cdots, y_k, y_{k+1}) = ((y_1, \cdots, y_k), y_{k+1})$.

我们显然有 $\Gamma_{k+1}(G)\subseteq(\Gamma_k(G), G)$. 为了证明另一方向的包含式，我们需要利用恒等式(10.2.1). 在(10.2.1.2)中令 $x=(a_1,\cdots,a_k)$, $y=(a_1,\cdots,a_k)^{-1}$, $z=a_{k+1}$. 那么 $1=(1,a_{k+1})=(a_1,\cdots,a_k,a_{k+1})^y((a_1,\cdots,a_k)^{-1},a_{k+1})$. 因而我们有 $((a_1,\cdots,a_k)^{-1},a_{k+1})\in\Gamma_{k+1}(G)$, 因为其他的项都属于 $\Gamma_{k+1}(G)$. 现在 $(\Gamma_k(G), G)$ 由元素 $(u_1u_2\cdots u_n, g)$ 生成，这里 $u_i=(a_1,\cdots,a_k)$ 或 $(a_1,\cdots,a_k)^{-1}$. 我们已经证明 $(u_i, g)\in\Gamma_{k+1}(G)$. 我们对 n 施行归纳法来证明 $(u_1u_2\cdots u_n,g)\in\Gamma_{k+1}(G)$. 在(10.2.1.2)中令 $x=u_1u_2\cdots u_{n-1}$, $y=u_n$, $z=g$, 我们有 $(u_1\cdots u_{n-1}u_n, g)=(u_1\cdots u_{n-1}, g)^{u_n}(u_n, g)$; 根据归纳假设，右边的两项都在 $\Gamma_{k+1}(G)$ 内. 因此我们证明了 $(\Gamma_k(G), G)\subseteq\Gamma_{k+1}(G)$, 这就证明了定理.

这个定理导出一个重要的推论.

推论 10.2.1. $\Gamma(G)/\Gamma_{k+1}(G)$ 在 $G/\Gamma_{k+1}(G)$ 的中心内.

我们也可以对于任意群 G 定义上中心序列.

$$Z_0=1\subseteq Z_1(G)\subseteq Z_2(G)\subseteq\cdots\subseteq Z_i(G)\subseteq Z_{i+1}(G)\subseteq\cdots,$$

这里我们按下列规则定义 $Z_{i+1}(G)$: $Z_{i+1}(G)/Z_i(G)$ 是 $G/Z_i(G)$ 的中心. 因为群的中心是特征子群(一般不是完全不变的), 所以 Z_i 是 G 的特征子群. 下面的定理说明为什么在我们所定义的中心序列之前附加“上”和“下”的原因.

如果在序列 $G=A_1\supseteq A_2\supseteq A_3\supseteq\cdots\supseteq A_{r+1}=1$ 中每个 A_i/A_{i+1} 都在 G/A_{i+1} 的中心内，则它叫做中心序列.

定理 10.2.2. 设 $G=A_1\supseteq A_2\supseteq A_3\supseteq\cdots\supseteq A_{r+1}=1$ 是 G 的中心序列. 那么 $A_i\supseteq\Gamma_i(G)$, $i=1,\cdots,r+1$, 和 $A_{r+1-j}\subseteq Z_j(G)$, $j=0,1,\cdots,r$.

证明. 我们有 $A_1=G=\Gamma_1(G)$. 假定 $A_i\supseteq\Gamma_i(G)$. 因为 A_i/A_{i+1} 在 G/A_{i+1} 的中心内，所以我们有 $(A_i,G)\subseteq A_{i+1}$. 于是 $\Gamma_{i+1}(G)=(\Gamma_i(G), G)\subseteq(A_i, G)\subseteq A_{i+1}$, 根据归纳法，这

就证明了对于所有 i, $A_i \supseteq \Gamma_i(G)$. 假定对于某个 i, $A_{r+1-i} \subseteq Z_i(G)$. 那么 $T = G/Z_i(G)$ 是 $U = G/A_{r+1-i}$ 的同态像，同态核是 $Z_i(G)/A_{r+1-i}$. 现在 A_{r-i}/A_{r+1-i} 包含在U的中心内，因而它在T内的同态像必定在T的中心内. 但是这个像是 $A_{r-1} \cup Z_i/Z_i$,而T的中心是 Z_{i+1}/Z_i. 因此 $A_{r-i} \subseteq A_{r-i} \cup Z_i \subseteq Z_{i+1}$,根据归纳法这就证明了定理.

下列推论是这个定理的一个结果:

推论 10.2.2. 在幂零群G内，上和下中心序列都有有限长度而且有相同的长度 c.

因为如果存在长度 r 的有限的中心序列，则定理指出上和下中心序列最多有长度 r. 又如果把这两个序列彼此比较，则我们的结论是没有一个能长于另一个. 因此它们有相同的长度 c, 这个 c 叫做幂零群的类. 类 1 的幂零群是阿贝尔群.

定理 10.2.3. 如果群 G 由元素 $x_1, \cdots, x_r$ 生成，则 $\Gamma_k(G)/\Gamma_{k+1}(G)$由简单换位子 $(y_1, y_2, \cdots, y_k)$取模 $\Gamma_{k+1}(G)$ 生成,这里这些 y 从 $x_1, \cdots, x_r$ 中选取而且不一定是不同的.

推论 10.2.3. 如果G由 r 个元素生成,则 $\Gamma_k(G)/\Gamma_{k+1}(G)$ 最多由 r^k 个元素生成.

证明. 我们对 k 施行归纳法,当 $k=1$ 时定理直接得出. 假定定理对于 $k-1$ 成立. $\Gamma_k(G)$ 由 $a_i \in G$ 的全体换位子 $C=(a_1, \cdots, a_{k-1}, a_k)$ 生成. 这时 $C=((a_1, \cdots, a_{k-1}), a_k)$ 而且 $(a_1, \cdots, a_{k-1}) \in \Gamma_{k-1}(G)$, 因而根据归纳假设 $(a_1, \cdots, a_{k-1}) = u_1^{\epsilon_1} u_2^{\epsilon_2} \cdots u_n^{\epsilon_n} w$, $\epsilon_i = \pm 1$, $u_1, \cdots, u_n$ 是形状 $(y_1, \cdots, y_{k-1})$的换位子而且这些 y 都是些 x,又 $w \in \Gamma_k(G)$. 于是 $C = (u_1^{\epsilon_1} u_2^{\epsilon_2} \cdots u_n^{\epsilon_n} w, a_k)$. 应用(10.2.1.2),我们有 $C = (u_1^{\epsilon_1} u_2^{\epsilon_2} \cdots u_n^{\epsilon_n}, a_k)(u_1^{\epsilon_1} u_2^{\epsilon_2} \cdots u_n^{\epsilon_n}, a_k, w)(w, a_k) \equiv (u_1^{\epsilon_1} u_2^{\epsilon_2} \cdots u_n^{\epsilon_n}, a_k) (\mathrm{mod}\,\Gamma_{k+1})$. 现在 $a_k = x_{i_1}^{\eta_1} \cdots x_{i_m}^{\eta_m}$, $\eta_j = \pm 1$, 而且因为这些 $u \in \Gamma_{k-1}$, 重复应用 (10.2.1.2) 和 (10.2.1.3) 而且取模 Γ_{k+1},我们得出 C 是换

位子 $(u_j^{\varepsilon_j}, x_{i_s}^{\eta_s})$ 的乘积. 因为从这些规则还得出 $(u^\varepsilon, x^\eta) \equiv (u, x)^{\varepsilon\eta} \pmod{\Gamma_{k+1}(G)}$,所以 $\Gamma_k(G)/\Gamma_{k+1}(G)$ 由换位子 (u, x) 取模 $\Gamma_{k+1}(G)$ 或 $(y_1, \cdots, y_{k-1}, x_{i_k})$ 取模 $\Gamma_{k+1}(G)$ 生成,这是我们希望证明的. 注意在这个定理中并未用到 r 的有限性.

下列定理几乎是上述定理的一个直接推论，它给出幂零群和超可解群之间的关系.

定理 10.2.4. 有限生成的幂零群是超可解的.

证明. 设 G 是有限生成的幂零群. 设它的下中心序列是

$$G = \Gamma_1(G) \supset \Gamma_2(G) \supset \cdots \supset \Gamma_c(G) \supset \Gamma_{c+1}(G) = 1.$$

因为 $\Gamma_c(G)$ 是有限生成的阿贝尔群，所以它是 m 个循环群的直积. 又因为 $\Gamma_c(G)$ 在 G 的中心内，它的任何子群在 G 内是正规的. 因而存在着链 $\Gamma_{c+1} = 1 \subset \{a_1\} \subset \{a_1, a_2\} \subset \cdots \subset \{a_1, a_2, \cdots, a_m\} = \Gamma_c(G)$，它们全都是 G 的正规子群，而且序列中相邻两个群的商群都是循环群. 同理,我们可以在 $\Gamma_{i+1}(G)$ 和 $\Gamma_i(G)$ 之间插进正规子群，使得相邻的两个群的商群是循环群. 用这个方法可以得到 G 的一个序列，它就决定 G 是超可解的.

推论 10.2.4. 有限生成的幂零群满足极大条件.

群 G 满足极大条件是指它没有子群的无限递开链. 这等价于 G 和 G 的每个子群都是有限生成的. 我们将在定理10.5.1里证明超可解群的每个子群是超可解的因而是有限生成的. 关于可解群的对应命题不成立. 例如如果 F 是具有两个生成元素 a 和 b 的自由群,则 F/F' 是可解群,但是 F'/F'' 有无限多个生成元素 $a^{-i}b^{-j}a^ib^j$.

10.3. 幂零群的理论

我们看到如果群 G 是类 c 的幂零群，则每个换位子 $(a_1,$

$\cdots, a_{c+1})$都是单位元素，而且反之，如果每个$(a_1,\cdots, a_{c+1})=1$，则G是类最多为c的幂零群. 我们把$(a_1,\cdots, a_{c+1})=1$对于所有$a_i\in G$这个性质说成G是c幂零的.

定理 10.3.1. 如果G是c幂零的，则G的每个子群和商群也是c幂零的.

证明. 如果G是c幂零的，则对于子群H当然更有$a_i\in H$的所有换位子$(a_1,\cdots, a_{c+1})$都是1，因而H是c幂零的. 又如果T是G的同态像，则$b_i\in T$的每个换位子$(b_1,\cdots, b_{c+1})$是G内的某个换位子$(a_1,\cdots, a_{c+1})$的同态像，因而它是单位元素，所以T是c幂零的.

下列定理涉及本身可能不是幂零的群G的幂零正规子群.

定理 10.3.2. 如果H和K是G的正规子群，而且H是c幂零的，K是d幂零的，则$H\cup K=HK$是$c+d$幂零的.

证明. $\Gamma_m(HK)$由$u_i\in HK$的所有换位子$(u_1, u_2,\cdots, u_m)$生成，因而$u_i=h_ik_i$, $h_i\in H$, $k_i\in K$. 我们可以断定$(u_1, u_2, \cdots, u_m)$是形状$w=(v_1, v_2,\cdots, v_m)$的换位子的乘积，这里每个v_i是一个$h\in H$或一个$k\in K$. $m=1$的情形是显然的. 假定这在$m-1$时成立. 那么应用(10.2.1.3)以及H和K的正规性，我们有

$$\begin{aligned}(u_1,\cdots, u_{m-1}, u_m) &= (w_1w_2\cdots w_t, h_mk_m)\\ &= (w_1\cdots w_t, k_m)(w_1\cdots w_t, h_m)^{k_m}\\ &= (w_1\cdots w_t, k_m)(w_1^{k_m}\cdots w_t^{k_m}, h_m^{k_m})\\ &= (w_1\cdots w_t, k_m)(w_1'\cdots w_t', h_m').\end{aligned}$$

同理，应用(10.2.1.2)，

$$\begin{aligned}(w_1\cdots w_t, k_m) &= (w_1, k_m)^{w_2\cdots w_t}(w_2\cdots w_t, k_m)\\ &= (w_1'', k_m'')(w_2\cdots w_t, k_m).\end{aligned}$$

这样继续下去，我们最后把$(u_1,\cdots, u_{m-1}, u_m)$表示成$(w,$

$h_m^{(i)}$) 和 (w, $k_m^{(i)}$) 的项的乘积，这些项就有形状 $(v_1, \cdots, v_m)$，这里每个 v 都是一个 h 或一个 k. 这样就用归纳法证明了我们的论断. 我们现在来证明 $\Gamma_{c+d+1}(HK)$ 由换位子 $(v_1, \cdots, v_{c+d+1})$ 生成，这里每个 v_i 是一个 h 或一个 k. 一般地我们有 $(v_1, \cdots, v_{t-1}, v_t) = (v_1, \cdots, v_{t-1}) v_t^{-1}(v_1, \cdots, v_{t-1})v_t$. 根据 $\Gamma_i(H)$ 在 HK 内的正规性，如果 $(v_1, \cdots, v_{t-1}) \in \Gamma_i(H)$，则当 v_t 是一个 k 时有 $(v_1, \cdots, v_t) \in \Gamma_i(H)$，而当 v_t 是一个 h 时有 $(v_1, \cdots, v_t) \in \Gamma_{i+1}(H)$. 因此，如果在 $(v_1, \cdots, v_{c+d+1})$ 中有 $c+1$ 个 h，则它属于 $\Gamma_{c+1}(H) = 1$，即它是单位元素. 否则在 $(v_1, \cdots, v_{c+d+1})$ 中至少有 $d+1$ 个 k，用同样论证得出它属于 $\Gamma_{d+1}(K) = 1$. 总之 $(v_1, \cdots, v_{c+d+1}) = 1$，因此 $H \cup K = HK$ 是 $c+d$ 幂零的.

定理 10.3.3. 如果群 G 是 c 幂零的，$H = H_0$ 是它的任何子群而且 H_{i+1} 是 H_i 在 G 内的正规化子，则 $H_c = G$.

证明. $H_0 \supseteq Z_0 = 1$ 是显然的. 我们用归纳法证明对于所有 m，$H_m \supseteq Z_m$. 假定 $H_i \supseteq Z_i$. 那么根据 Z_{i+1} 的定义，对于任何 $z_{i+1} \in Z_{i+1}$ 和 $g \in G$，我们有 $z_{i+1}^{-1} g^{-1} z_{i+1} g = z_i \in Z_i$，因而当 $g^{-1} = h_i \in H_i$ 时我们有 $z_{i+1}^{-1} h_i z_{i+1} = z_i h_i \in H_i$，所以 Z_{i+1} 属于 H_i 的正规化，即 $H_{i+1} \supseteq Z_{i+1}$，这就用归纳法证明了我们的论断. 而因为 $Z_c = G$，我们必须有 $H_c = G$.

推论 10.3.1. 幂零群的每个真子群是它的正规化子的真子群.

推论 10.3.2. 幂零群的每个极大子群是正规的、指数为素数的，而且包含着导出群.

设 M 是幂零群 G 的极大子群. 因为 $N_G(M)$ 真包含 M，我们必须有 $N_G(M) = G$，即 $M \triangleleft G$. 于是根据 M 的极大性，G/M 不包含真子群，因而它必定是素数阶的循环群. 因此 M 的指数是素数. 又因为 G/M 是阿贝尔群，M 包含导出群 G'.

推论 10.3.3. 如果H是幂零群G的子群，$G = G'H$，则$H = G$.

这时如果$H \neq G$，则根据定理，当$H = H_0$和$H_{i+1} = H_i Z_{i+1}$时就有每个H_i在H_{i+1}内是正规的. 如果$H_j \neq G$，但是$H_{j+1} = G$，则H_j是G的正规真子群而且G/H_j是阿贝尔群，因而$H_j \supseteq G'$. 于是$HG' \subseteq H_j G' = H_j \neq G$而与假设矛盾. 因此我们必须有$H = G$，这就证明了这个推论. 注意在这里并未假定$G$具有极大子群.

定理 10.3.4. 有限p群是幂零的. 有限群是幂零的，必要而且只要它是它的西罗子群的直积.

证明. 根据定理 4.3.1，每个有限p群P具有不是单位元素群的中心. 因此P的上中心序列以整个群结尾，即P是幂零的. 同样的论证对于有限p群的直积也成立. 现在假定G是任何有限的幂零群，而且设P是G的西罗p子群. 那么根据定理 4.2.4，$N_G(P)$是它自己的正规化子，因而根据推论 10.3.1，$N_G(P)$不能是G的真子群. 因此$P \triangleleft G$. 由于G的每个西罗子群都是正规的，G必定是它的西罗子群的直积.

推论 10.3.4 (维兰德). 有限群是幂零的，必要而且只要它的极大子群是正规的.

因为根据定理 10.3.3 的推论 10.3.2，幂零群的极大子群是正规的. 另一方面，根据定理 4.2.4，当P是西罗p子群时，$N_G(P)$不能包含在G的正规真子群内. 因此如果极大子群是正规的，则$P \triangleleft G$，因而G是它的西罗子群的直积.

定理 10.3.5. 如果X, Y, Z是群G的子群，而且K是G的包含(Y, Z, X)和(Z, X, Y)的正规子群，则K也包含(X, Y, Z).

证明. 从(10.2.1.4)我们有

$$(x, y, z) = ((z, x^{-1}, y^{-1})^{xy})^{-1}((y^{-1}, z^{-1}, x)^{zy})^{-1}.$$

这就能得出所要的结论.

定理 10.3.6. 如果 $H = H_0 \supseteq H_1 \supseteq \cdots$ 是群 G 的正规子群，$(H_{i-1}, L) \subseteq H_i$ 对于所有的 i 和子群 L，则 $(H_i, \Gamma_j(L)) \subseteq H_{i+j}$.

推论 10.3.5. $(\Gamma_i(G), \Gamma_j(G)) \subseteq \Gamma_{i+j}(G)$.

证明. 我们对 j 施行归纳法，定理的假设已经包括了 $j = 1$ 的情形. 假定对于所有的 i 都有 $(H_i, \Gamma_{j-1}(L)) \subseteq H_{i+j-1}$. 那么根据归纳假设，$(L, H_i, \Gamma_{j-1}(L)) \subseteq (H_{i+1}, \Gamma_{j-1}(L)) \subseteq H_{i+j}$ 而且 $(H_i, \Gamma_{j-1}(L), L) \subseteq (H_{i+j-1}, L) \subseteq H_{i+j}$. 因为 $(\Gamma_{j-1}(L), L) = \Gamma_j(L)$，我们可以应用定理 10.3.5 而得出

$$(H_i, \Gamma_j(L)) = (H_i, (\Gamma_{j-1}(L), L))$$
$$= (\Gamma_{j-1}(L), L, H_i) \subseteq H_{i+j},$$

这就是定理的结论.

10.4. 群的弗拉梯尼子群

设 G 是任意的群. 我们以下列方式定义 G 的弗拉梯尼子群 Φ: $\Phi = G \bigcap_M M$，这里 M 遍历 G 的极大子群，如果 G 具有极大子群. 因此 $\Phi = G$ 必要而且只要 G 不具有极大子群. 因为 G 的任何自同构更换它的极大子群，所以弗拉梯尼子群显然是特征子群.

弗拉梯尼子群与 G 的生成元素组有密切的关系. 它由 G 中在下列意义下称为非生成元素的元素组成.

定义. G 的元素 x 叫做 G 的非生成元素，假如对于 G 的子集 T 有 $G = \{T, x\}$，则 $G = \{T\}$.

注意我们要求 $\{T, x\} = \{T\}$ 对于每个使 $\{T, x\} = G$ 的子集 T. 这时如果 $G \neq 1$，则 1 当然是非生成元素.

定理 10.4.1. 如果群G不是单位元素群，则它的弗拉梯尼子群Φ由G的全体非生成元素组成.

证明. 设x是G的元素. 如果存在不包含x的极大子群M，则群$\{M, x\}$真包含M，而由于M是极大的，我们必须有$\{M, x\}=G$. 但是这时$\{M\}=M\neq G$. 因而x在$\{M, x\}=G$中是必要的生成元素. 因此G的非生成元素属于每个极大子群,所以每个非生成元素都属于$\Phi=G\bigcap\limits_{M} M$. 反之，我们还需要证明，如果$u\in\Phi$，则$u$是$G$的非生成元素. 根据假设$G\neq 1$,因而1当然是非生成元素.

现在假定对于G的子集T，$G=\{T, u\}$. 我们来证明如果$\{T\}=H\neq G$，则就将导出矛盾. 现在如果$H\neq G$,则我们不能有$u\in H$,因为在这情形下$H=\{H, u\}\supseteq\{T, u\}=G$. 因此$u\notin H$. 于是根据左恩引理,存在子群$K\supseteq H$，对于$u\notin K$的性质说是极大的.现在$\{K, u\}\supseteq\{T, u\}=G$,因而$\{K, u\}=G$. 但是根据$K$的选取,真包含$K$的任何群必须包含$u$. 因此$K=M$是不包含$u$的极大子群，这就违反了$u\in\Phi=G\bigcap\limits_{M} M$. 因而必定有$\{T\}=G$,所以每个$u\in\Phi$是$G$的非生成元素.

定理 10.4.2. 有限群的弗拉梯尼子群是幂零的.

设G是有限群而且Φ是它的弗拉梯尼子群. 设P是Φ的西罗p子群. Φ作为G的特征子群是正规子群. 因而P在G内的每个共轭者都在Φ内,因为它们都是Φ的西罗p子群,所以是P在Φ内的共轭者. 因此P在Φ内的共轭者数与在G内的相同,所以$[G:N_G(P)]=[\Phi:N_\Phi(P)]$. 但是$[G:N_\Phi(P)]=[G:\Phi][\Phi:N_\Phi(P)]=[G:N_G(P)][N_G(P):N_\Phi(P)]$,因而$[G:\Phi]=[N_G(P):N_\Phi(P)]$. 注意到$N_\Phi(P)=N_G(P)\cap\Phi$而且应用定理1.5.5中关于指数的不等式,就能得出

$$[N_G(P)\cup\Phi:\Phi]\geqslant[N_G(P):N_G(P)\cap\Phi]=[G:\Phi].$$

由此可知 $N_G(P)\cup\Phi=G$. 现在因为 $G=\{N_G(P),\Phi\}$,所以每次移去 Φ 的一个元素,由于 Φ 是有限的,我们还将有

$$G=\{N_G(P)\}=N_G(P).$$

于是 $P\lhd G$, 当然更有 $P\lhd\Phi$. 因为 Φ 的每个西罗子群是正规的, Φ 必定是它的西罗子群的直积,因而它是幂零群.

定理 10.4.3. 幂零群的弗拉梯尼子群包含导出群.

证明. 根据推论 10.3.3,如果 G 是幂零的而且 $G=HG'$, 则 $G=H$. 这说明 G' 可以从 G 的任何生成组删去, 因而得出 $\Phi\supseteq G'$. 逆命题对于有限群成立.

定理 10.4.4 (维兰德). 如果有限群 G 的弗拉梯尼子群包含导出群 G', 则 G 是幂零的.

证明. 设 P 是 G 的西罗子群. 如果 $N_G(P)=H\neq G$,则 H 包含在 G 的某个极大子群 M 内. 然而 $M\supseteq\Phi$, 而且根据假设, $\Phi\supseteq G'$. 因为 G/G' 是阿贝尔群,所以 M 是 G 的正规子群. 另一方面,根据定理 4.2.4,因为 $M\supseteq N_G(P)$, M 是它自己的正规化子. 这是一个矛盾, 因而我们必须有 $N_G(P)=G$. G 的西罗子群都是正规的,因而 G 是它们的直积,即是幂零的.

10.5. 超可解群

定理 10.5.1. 超可解群的子群和商群是超可解的.

证明. 设 G 是超可解群而且

$$G=A_0\supset A_1\supset A_2\supset\cdots\supset A_r=1$$

是正规序列, 其中每个 A_{i-1}/A_i 都是循环群. 那么对于商群 $G/K=T$, A_i 的同态像 B_i 组成正规序列

$$T=B_0\supseteq B_1\supseteq B_2\supseteq\cdots\supseteq B_r=1,$$

这里在把重复的群删去后, 对于相邻的项 B_{i-1} 和 B_i 就将有循环的商群 B_{i-1}/B_i,因为循环群的同态像是循环群或单位元

素群．对于子群 H，取 $H = C_0 \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_r = 1$，这里 $C_i = H \cap A_i$．对于每个 i，$H \cap A_i$ 在 H 内是正规的，而且根据定理 2.4.1，我们有

$$C_i / C_{i+1} = H \cap A_i / H \cap A_{i+1} \cong A_{i+1} \cup (H \cap A_i) / A_{i+1}.$$

但是右端是 A_i / A_{i+1} 的子群因而是循环群或单位元素群．因此 C_i / C_{i+1} 是循环群或单位元素群，所以 H 是超可解的．

推论 10.5.1. 超可解群满足极大条件．

超可解群是有限生成的，因而根据定理 10.5.1，它的子群也是有限生成的，所以极大条件满足．

定理 10.5.2. 超可解群 G 具有正规序列

$$G = B_0 \supset B_1 \supset B_2 \supset \cdots \supset B_k = 1,$$

其中每个商群 B_{i-1}/B_i 是无限循环群或素数阶循环群．

证明．设 $G = A_0 \supset A_1 \supset A_2 \supset \cdots \supset A_r = 1$ 是正规序列，其中 A_{i-1}/A_i 是循环群．如果 A_{i-1}/A_i 有有限的阶 $p_1 p_2 \cdots p_s$，这里 $p_1, p_2, \cdots, p_s$ 是素数（不必须是不同的），则 A_{i-1}/A_i 具有阶为 $p_1, p_1 p_2, \cdots, p_1 \cdots p_{s-1}$ 的唯一循环子群而且这些都是特征子群．因此在 A_{i-1} 和 A_i 之间的 $s-1$ 个对应的子群在 G 内是正规的，而且相邻的群的商群是素数阶循环群．用这个方法加细每个有限阶的商群 A_{i-1}/A_i，就得出定理中的正规序列，其中每个商群是无限循环群或素数阶循环群．

这个定理还可以进一步加强而按素数的大小来重新排列素数阶商群．

定理 10.5.3. 超可解群 G 具有正规序列

$$G = C_0 \supset C_1 \supset C_2 \supset \cdots \supset C_k = 1,$$

其中每个 C_{i-1}/C_i 是无限循环群或素数阶循环群，而且对于具有素数阶 p_i 和 p_{i+1} 的 C_{i-1}/C_i 和 C_i/C_{i+1}，我们有 $p_i \leqslant p_{i+1}$．

证明．取定理 10.5.2 中给出的序列

$$G = B_0 \supset B_1 \supset B_2 \supset \cdots \supset B_k = 1.$$

如果 B_{i-1}/B_i 和 B_i/B_{i+1} 的阶分别是素数 q 和 p 而且 $q > p$，则 B_{i-1}/B_{i+1} 的阶是 pq 而且 $p < q$，它有 q 阶的特征子群，这子群的逆像 B_i^* 在 G 内是正规的．如果我们把 B_i 换成 B_i^*，则 B_{i-1}/B_i^* 的阶是 p 而 B_i^*/B_{i+1} 的阶是 q．继续这个步骤，它并不改变序列的长度，我们最终得到一个序列，在其中相邻的素数阶商群的阶不会递增，这就是定理所要的．

推论 10.5.2. 如果 G 是阶为 $p_1p_2\cdots p_r$ 的有限超可解群，这里 $p_1 \leqslant p_2 \leqslant \cdots \leqslant p_r$ 都是素数，则 G 具有主序列

$$G = A_0 \supset A_1 \supset \cdots \supset A_r = 1,$$

其中 A_{i-1}/A_i 的阶是 p_i.

定理 10.5.4. 超可解群的导出群是幂零的.

证明. 设 $G = A_0 \supset A_1 \supset \cdots \supset A_r = 1$ 是 G 的正规序列，其中 A_{i-1}/A_i 是循环群．记 $H_i = G' \cap A_i$．那么

$$G' = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_r = 1$$

是正规序列．而且这序列中不同的项 K_i 组成序列

$$G' = K_0 \supset K_1 \supset \cdots \supset K_s = 1,$$

其中 K_{i-1}/K_i 是循环群．我们来断定这些 K 组成 G' 的中心序列．每个 K_i 是 G 中正规子群的交，因此在 G 内是正规的．这时在 G/K_i 内 K_{i-1}/K_i 是循环的正规子群，用 G/K_i 的元素作变形导出循环群 K_{i-1}/K_i 的自同构．然而循环群的自同构组成阿贝尔群，所以 G/K_i 的两个元素导出 K_{i-1}/K_i 的可交换的自同构．于是任何两个元素的换位子 $x^{-1}y^{-1}xy$ 导出 K_{i-1}/K_i 的恒同自同构．这说明 K_{i-1}/K_i 属于 G'/K_i 的中心，因而这些 K 组成 G' 的中心序列，所以 G' 是幂零的.

在超可解群内由任意子群组成的链具有一个有趣的性质．我们说 H_2 在 H_1 内的指数是 ∞^1，假如 $H_1 = \sum_x H_2a^x$ 对于某个元素 a，这里 x 遍历从 $-\infty$ 到 $+\infty$ 的全体整数．因而如

果 $A_j \lhd A_{j-1}$ 而且 A_{j-1}/A_j 是无限循环群，则 A_j 在 A_{j-1} 内的指数是 ∞^1，因为我们可以在作为循环群 A_{j-1}/A_j 的生成元素的 A_j 的傍系内取任意元素作为 a. 但是在 H_1 内有指数 ∞^1 的 H_2 可以在 H_1 内不是正规的.

定理 10.5.5. 在超可解群 G 内，子群的任意链

$$G = M_0 \supset M_1 \supset M_2 \supset \cdots \supset M_s = 1$$

可以插入下列群而加细:

$$M_{i-1} = M_{i,0} \supset M_{i,1} \supset \cdots \supset M_{i,t} = M_i,$$

$$t = t(i), \qquad i = 1, \cdots, s,$$

使得 $M_{i,j}$ 在 $M_{i,j-1}$ 内的指数是素数或 ∞^1.

证明. 因为 M_1 是超可解的，所以只要证明已知序列可以在 $G = M_0$ 和 M_1 之间插入若干项而加细成具有所要的性质. 然后依次对 $M_1, \cdots, M_{s-1}$ 重复这个论证，就能加细整个序列.

设 $G = A_0 \supset A_1 \supset A_2 \supset \cdots \supset A_r = 1$ 是 G 的正规序列，这里每个 A_{i-1}/A_i 是素数阶或无限阶的循环群. 当然有 $M_1 \supseteq A_r = 1$ 和 $M_1 \not\supseteq A_0 = G$. 因此对于 $1, \cdots, r$ 中的某个 i 有 $M_1 \supseteq A_i$ 和 $M_1 \not\supseteq A_{i-1}$. 我们考虑两种情形: (1) A_{i-1}/A_i 是素数阶的，(2) A_{i-1}/A_i 是无限循环群.

情形 1. A_{i-1}/A_i 是素数阶的. 这时 $A_{i-1} \supset M_1 \cap A_{i-1} \supseteq A_i$. 因为 A_i 在 A_{i-1} 内的指数是素数，在 A_i 和 A_{i-1} 之间不能存在子群. 因此 $M_1 \cap A_{i-1} = A_i$. 如果 $A_{i-1} = \sum_x A_i a^x$, $x = 0, \cdots, p-1$，则 $M_1 \cup A_{i-1} = M_1 A_{i-1} = M_1^*$，而 $M_1^* = \sum_x M_1 a^x$, $x = 0, 1, \cdots, p-1$, 因为 M_1 包含 A_i 而不包含 a，但是 $a^p \in A_i$. 这时 M_1 在 M_1^* 内的指数是素数而且 $M_1^* \supseteq A_{i-1}$.

情形 2. A_{i-1}/A_i 是无限循环群. 这时 $A_{i-1} \supset M_1 \cap A_{i-1} \supseteq A_i$. 由于 A_{i-1}/A_i 的每个子群都是特征子群，因而 $M_1 \cap A_{i-1}$

是 G 的正规子群．如果 $M_1\cap A_{i-1}=A_i$ 而且

$$A_{i-1}=\sum_x A_i a^x,$$

则令 $M_1^*=M_1\cup A_{i-1}=M_1A_{i-1}=\sum_x M_1a^x$，于是 M_1 在 M_1^* 内有指数 ∞^1，因为 M_1 包含 A_i 而不包含元素 a 的方幂．又如果 $M_1\cap A_{i-1}\supset A_i$，则因为无限循环群的每个子群是有限指数的，所以 $M_1\cap A_{i-1}$ 在 A_{i-1} 内的指数有限．因而在我们的正规序列内可以在 A_{i-1} 和 $M_1\cap A_{i-1}$ 之间插入若干项，使得后一项在前一项内的指数是素数，于是像在情形 1 里那样，找出 M_1^* 使 M_1 在其中有素数指数．重复这个构造，我们找到链 $M_1\subset M_1^*\subset M_1^{**}\subset\cdots\subset M_1^{(u)}$，使每个群在后一个中有素数指数而且 $M_1^{(u)}\supseteq A_{i-1}$．

继续这个构造，在有限步后将达到 $M_1^{(v)}\supseteq A_0=G$，因而找出了定理中所需要的在 G 和 M_1 之间的加细．前面已经说过，同样的步骤可以给出关于整个链的所要的加细．

对于有限群，这个定理成为下列有趣的形式．

定理 10.5.6. 在有限的超可解群 G 内，子群的所有极大链具有相同的长度，当 G 的阶是 $p_1p_2\cdots p_r$ 时，这里的 p 是素数，但不必须是不同的，这个长度就是 r 这个数．

证明．根据前一个定理，在极大链中每个子群在后一个子群中的指数都是素数，因而极大链的长度是 r．

推论 10.5.1. 有限超可解群的每一个极大子群都是素数指数的．

最先由胡帕特（Huppert [1]）证明的可注意的事实是：这个推论的逆命题也成立．为此我们必须用到在第十六章里证明的关于群表示的若干定理．我们先来证明 P. 赫尔的一个未发表的定理．

定理 10.5.7（P. 赫尔）． 如果 G 是有限群，具有性质

(M):它的所有极大子群的指数是素数或素数的平方，那么G是可解的.

证明. 我们对G的阶施行归纳法. 设p是整除这个阶的最大素数，S是G的西罗p子群，N是它在G内的正规化子. 如果$N=G$，则S在G内是正规的而且G/S具有性质(M)，因而根据归纳假设，G/S是可解的. S是p群，因而G是可解的. 否则当$N\subset G$时，取G的包含N的极大子群H. 在H内像在G内一样，N是S的正规化子，因而根据第三个西罗定理，$[G:N]=1+k_1p$，$[H:N]=1+k_2p$，这分别是在G和H内的西罗p子群的个数. 因此$[G:H]=1+kp$. 但是根据假设，对于某个素数$q[G:H]=q$或q^2；而且显然有$q<p$，$k>0$. 因此$kp=q^2-1=(q-1)(q+1)$. 因为$p\geqslant q+1$，我们必须有$p=q+1$. 唯一的可能是$p=3$和$q=2$，因而G的阶有形状2^a3^b. 根据定理16.8.7，G是可解的.

定理 10.5.8 (胡帕特). 假定G是有限群，具有性质(M^1)，它的全体极大子群的指数都是素数. 那么G是超可解群.

证明. 如果定理不成立，G具有性质(M^1)而不是超可解群，而且它是具有这两个性质的群中阶最小的. 那么根据定理10.5.8，G是可解的. 设N是G的极小正规子群，它的阶是p^α，p是素数. 根据G的极小性，G/N是超可解的，因而在G的主序列的商群中，只有N是非循环的. 我们有结论：N是G的唯一极小正规子群. 设H/N是G/N的极小正规子群. 存在两种情形：(1) $[H:N]=p$，(2) $[H/N]=q$，q是与p不同的素数. 在(1)中H必定是阿贝尔群，因为否则将有$1\subset H'\subset N$而且N'在G内是正规的. 由于$\alpha>1$，H不能有p^2阶元素，因为这将使N包含H的p阶特征子群，这将导出同样的结论. 因此H是初等阿贝尔群.

现在以自然的方式把G表示成H的自同构群，即表示成

模 p 的 $\alpha+1$ 次线性变换的群(因为H的阶是 $p^{\alpha+1}$). 设K是全体这种元素 $a \in G$ 的集合，对于 $x \in H$ 有 $a^{-1}xa = x^m$，这里 $m = m(a)$ 不依赖于 x. 再设L是H在G内的中心化子. 那么K/L 包含在 G/L 的中心内. 又 $K \subset G$，因为N是G的唯一极小正规子群，而且H的每个子群在 K 内是正规的. 设 M/K是 G/K 的极小正规子群. 如果$[M:K]=p$,就将有 M/L 是K/L(它的阶与 p 互素而且在 G/L 的中心内)与一个 p 阶群$\{L, a\}/L$ 的直积，而且 $M_1 = \{L, a\}$ 在G内是正规的. 因为换位子群$(N, L) = 1$而且 $[M_1:L]=p$,所以N包含 M_1 的中心的$\neq 1$ 的元素. M_1的中心是G的正规子群,因而根据N的极小性,N在 M_1 的中心内而且$(M_1, N) = 1$. 如果 $H=\{N, b\}$,则群 (H, M_1) 是 p 阶的而且由$(a, b) = c \in N$ $(c \neq 1)$ 生成. 然而这个群在G内是正规的,因而N不能是G的极小正规子群.

因此 $[M:K] = q$，q 是与 p 不同的素数，因而 M/L 的阶与 p 互素. 根据完全可约性定理(定理 16.3.1)，由此得出 $H = N \times P$，这里P是在M内正规的 p 阶群. P 在G内的共轭者是在M内正规的 p 阶子群，因而它们的并Q是G的正规子群. 因为N是G的唯一的极小正规子群而且 $Q \neq N$，所以 $Q = H$. 因为P不在N内，P的共轭者也不在N内. 设 $P = \{b\}$，$b^p = 1$,又如果 $P_i \neq P$ 是P的任意共轭者,则 $PP_i \cap N = R$,这时因为 $[H:N] = p$, R是 p 阶的. 我们可以取P_i的生成元素 c，使得 $P_i = \{c\}$，$R = \{bc\}$. 因为 P, P_i, R 都是M的正规子群，所以对于M的任何 a，$a^{-1}ba = b^m$，$a^{-1}ca = c^n$，$a^{-1}(bc)a = (bc)^t$. 于是 $(bc)^t = b^m c^n$，因而 $t = n = m$. 由于P_i是P的任意共轭者,所以对于任何 $x \in H$,我们有 $a^{-1}xa = x^m$,这里 $m = m(a)$ 与 x 无关. 因此 $M \subseteq K$，这是一个矛盾. 总之情形 (1) 不能发生.

情形 (2) 可以立刻解决．如果 $[H:N]=q$ 不同于 p，设 Q 是 H 的西罗 q 子群，T 是 Q 在 G 内的正规化子．Q 在 G 内的任何共轭者属于 H，因而是 Q 被 N 的元素作用而得出的共轭者．因此 $G=NT$．于是 $N\cap T$ 在 G 内是正规的．但是 $T\not\supseteq N$，因为这将使 $T=G$ 因而 Q 在 G 内是正规的．因此 $N\cap T=1$，$[G:T]=p^{\alpha}$ 但是 T 是 G 的极大子群，因为在 $T\subset T_1\subset G$ 时将有 $1\subset T_1\cap N\subset N$ 而且 $T_1\cap N$ 在 G 内是正规的．于是 G 具有指数不是素数的极大子群而与假设矛盾．

习　　题

1．设 $I^{(1)}=I^{(1)}(G)$ 是 G 的内自同构群而且 $I^{(n)}$ 是 $I^{(n-1)}$ 的内自同构群．当序列 $G, I^{(1)}, I^{(2)}, \cdots$ 中有单位元素群时，证明 G 是幂零的．

2．设 G 是满足极大条件的群．当 G 的自同构群 $A(G)$ 是超可解群时，证明 G 是超可解的．

3．设 a 和 b 是幂零群 G 的元素，$a^m=b^n=1$，$(m,n)=1$．令 $w=a^{-1}b^{-1}ab$．证明如果 $w\in\Gamma_i(G)$，则 $w^m\in\Gamma_{i+1}(G)$，$w^n\in\Gamma_{i+1}(G)$，因而 $w\in\Gamma_{i+1}(G)$．因此有结论 $w=1$，$ba=ab$．

4．证明第八章习题 2 的逆命题，即：如果 G 是有限的幂零群，而且 $p_1, p_2, \cdots, p_s$ 是乘积等于 G 的阶的任意地排列的素数，则 G 具有合成序列 $G=A_0\supset A_1\supset\cdots\supset A_s=1$，这里 A_{i-1}/A_i 的阶是 p_i．

5．设 G 是 p 群而且 $\Gamma_3(G)=1$．证明，如果 p^m 是 $G/\Gamma_2(G)$ 的元素的最高的阶，则 $\Gamma_2(G)$ 的元素不会有比 p^m 高的阶．

第十一章　基本换位子

11.1. 集积过程

我们考虑形式的字或串 $b_1b_2\cdots b_n$，这里每个 b 都是字母 $x_1, x_2, \cdots, x_r$ 中的一个．我们还用下列规则导入形式的换位子 c_j 和权 $\omega(c_j)$：

1）$c_i = x_i, i = 1, \cdots, r$ 是权 1 的换位子；即 $\omega(x_i) = 1$.

2）如果 c_i 和 c_j 是换位子，则 $c_k = (c_i, c_j)$ 是换位子，而且 $\omega(c_k) = \omega(c_i) + \omega(c_j)$.

注意这些定义对于任何给定的权只产生有限个换位子．我们将用下指标表出换位子的顺序，编排 $c_i = x_i$，$i = 1, \cdots, r$，然后以权的次序来编排，但是对于同一权的换位子给以任意的顺序．

换位子的串 $c_{i_1}\cdots c_{i_m}$ 当 $i_1 \leqslant i_2 \leqslant \cdots \leqslant i_m$，即当换位子从左到右都按顺序排时，叫做集积的．任意的换位子串

$$c_{i_1}\cdots c_{i_m}c_{i_{m+1}}\cdots c_{i_n} \tag{11.1.1}$$

一般会有集积的部分 $c_{i_1}\cdots c_{i_m}$，只要 $i_1 \leqslant \cdots \leqslant i_m$ 而且 $i_m \leqslant i_j$，$j = m + 1, \cdots, n$，也会有未集积的部分 $c_{i_{m+1}}\cdots c_{i_n}$，这里 i_{m+1} 不是 i_j，$j = m + 1, \cdots, n$ 中最小的．当 i_1 不是最小的下指标时，串 $c_{i_1}\cdots c_{i_n}$ 没有集积的部分．

我们来定义换位子串的集积过程．如果 c_u 是在未集积部分中的最先的换位子，而且 $c_{i_j} = c_u$ 是最左的未集积的 c_u，我们把

$$c_{i_1}\cdots c_{i_m}\cdots c_{i_{j-1}}c_{i_j}\cdots c_{i_n}$$

换成

$$c_{i_1}\cdots c_{i_m}\cdots c_{i_j}c_{i_{j-1}}(c_{i_{j-1}}, c_{i_j})\cdots c_{i_n}.$$

结果把 c_{i_j} 移向左边而且导入了新的换位子 $(c_{i_{j-1}}, c_{i_j})$，按照它的权它一定在 c_{i_j} 之后．因而 c_{i_j} 仍然是未集积部分的最先的换位子．在一定的步数以后，c_{i_j} 将移到第 $m+1$ 个位置，因而就成为集积部分的一部分．由于在每一步都要导入一个新的换位子，这个过程一般不会终止．

设 $x_1, \cdots, x_r$ 是群 F 的生成元素（而且我们主要讨论 F 是具有这些生成元素的自由群的情形），再设换位子 $(u, v)=u^{-1}v^{-1}uv$．那么由于

$$c_{i_{j-1}}c_{i_j} = c_{i_j}c_{i_{j-1}}(c_{i_{j-1}}, c_{i_j}), \qquad (11.1.2)$$

因而集积过程不会改变由字表出的群的元素．但是集积过程有定义的并非 F 的全部元素，而只是正的字，即能表成生成元素的乘积而不用到生成元素的任何逆的元素．下面将会消除这个缺陷．

在把集积过积运用到正的字时，并非全部换位子都会出现．例如 (x_2, x_1) 会出现而 (x_1, x_2) 则否，因为 x_1 在 x_2 之前被集积了．真正会出现的换位子叫做基本换位子．我们来给出由 $x_1, \cdots, x_r$ 生成的群 F 的基本换位子的形式定义．

基本换位子的定义:

1）$c_i=x_i$, $i=1,\cdots, r$ 是权 1 的基本换位子，$\omega(x_i)=1$.

2）在定义了权小于 n 的基本换位子以后，权 n 的基本换位子是 $c_k=(c_i, c_j)$，这里

(a) c_i 和 c_j 是基本的而且 $\omega(c_i)+\omega(c_j)=n$,

(b) $c_i > c_j$，又如果 $c_i=(c_s, c_t)$，则 $c_j \geqslant c_t$.

3）权 n 的换位子在权小于 n 的换位子之后，而且彼此任意地排成顺序．基本换位子总编成号码使得它们的顺序由下指标表出．

我们注意到，当换位子按权编排，而在同权时任意编排，那么在把集积过程运用到正的字时，只会产生基本换位子．因为在替换

$$c_u c_v = c_v c_u (c_u, c_v) \qquad (11.1.3)$$

中，我们在 c_u 之前集积 c_v，因而 $c_u > c_v$，又如果 $c_u = (c_s, c_t)$，则我们在集积这个 c_v 之前已经集积了 c_t，因而 $c_v \geqslant c_t$。

我们现在来证明，在对 $\Gamma_{k+1}(F)$ 取模时，这里 $\Gamma_{k+1}(F)$ 是 F 的下中心序列的第 $k+1$ 项（k 是任意的），以后把它记做 Γ_{k+1}，F 的任意元素可以写成

$$f = c_1^{e_1} c_2^{e_2} \cdots c_t^{e_t} (\mathrm{mod}\ F_{k+1}), \qquad (11.1.4)$$

这里 $c_1, \cdots, c_t$ 是权为 $1, 2, \cdots, k$ 的基本换位子．在集积过程中有

$$vu = uv(v, u), \qquad (11.1.5)$$

这里 u, v 和 (v, u) 都是基本换位子．我们还必须考虑集积在 vu^{-1}, $v^{-1}u^{-1}$ 和 $v^{-1}u$ 中的 u 或 u^{-1}．因为 $vu^{-1} = u^{-1}v(v, u^{-1})$，而且从 (10.2.1.3) 有

$$1 = (v, uu^{-1}) = (v, u^{-1})(v, u)(v, u, u^{-1}), \qquad (11.1.6)$$

因而 $(v, u^{-1}) = (v, u, u^{-1})^{-1}(v, u)^{-1}$．同理，$(v, u, u^{-1}) = (v, u, u, u^{-1})^{-1}(v, u, u)^{-1}$．记 $v_0 = v$，$v_{t+1} = (v_t, u)$，我们有

$$\begin{aligned}(v, u^{-1}) &= (v_1, u^{-1})^{-1} v_1^{-1} \\ &= v_2 (v_2, u^{-1}) v_1^{-1} \\ &= v_2 v_4 \cdots v_5^{-1} v_3^{-1} v_1^{-1} (\mathrm{mod}\ F_{k+1}),\end{aligned} \qquad (11.1.7)$$

而且我们注意到，如果 $v_1 = (v, u)$ 是基本的，则 $v_2, v_3, \cdots$ 也是基本的．取模 F_{k+1}，我们可以抹去 (v_s, u^{-1})，只要 s 大到使它有权 $k+1$ 或更高些．因此作为集积的一步，我们有

$$vu^{-1} = u^{-1}v \cdot v_2 v_4 \cdots v_5^{-1} v_3^{-1} v_1^{-1} (\mathrm{mod}\ F_{k+1}). \qquad (11.1.8)$$

同理，$v^{-1}u = uv^{-1}(v^{-1}, u)$，又从 (10.2.1.2)，$1 = (vv^{-1}, u) =$

$(v, u)(v, u, v^{-1})(v^{-1}, u)$，因而如果 $w_1 = (v, u)$，$w_{i+1} = (w_i, v)$，则就有

$$v^{-1}u = uv^{-1}w_2w_4\cdots w_3^{-1}w_1^{-1}(\text{mod } F_{k+1}). \qquad (11.1.9)$$

又 $v^{-1}u^{-1} = u^{-1}(uvu^{-1})^{-1}$，而且根据 (11.1.8)，

$$uvu^{-1} = v \cdot v_2v_4\cdots v_5^{-1}v_3^{-1}v_1^{-1}(\text{mod } F_{k+1}), \qquad (11.1.10)$$

因而

$$v^{-1}u^{-1} = u^{-1}v_1v_3v_5\cdots v_4^{-1}v_2^{-1}v^{-1}(\text{mod} F_{k+1}). \qquad (11.1.11)$$

重复应用 (11.1.5)，(11.1.8)，(11.1.9)，(11.1.11)，就能导出以一系列基本换位子来表示任意元素 f 的表示式 (11.1.4).

如果 F 是由 $x_1, x_2, \cdots, x_r$ 生成的自由群，则对于给定的基本换位子序列，我们将在 § 11.2 中证明表达式 (11.1.4) 是唯一的. 特别地，权 k 的基本换位子是 F_k/F_{k+1} 的自由基底，因而它是自由阿贝尔群. 这就是把基本这个词加到这些换位子上的原因.

11.2. 维特公式. 基底定理

假定给了由生成元素 $x_1, x_2, \cdots, x_r$ 组成的基本换位子的序列 $c_1, c_2, \cdots$. 我们把基本换位子的乘积

$$c_{i_1}c_{i_2}\cdots c_{i_n} \qquad (11.2.1)$$

叫做基本乘积，如果它有集积好的顺序，即 $i_1 \leqslant i_2 \leqslant \cdots \leqslant i_n$. 对于换位子的任意乘积 $p = a_1a_2\cdots a_n$，我们定义权 $\omega(p)$ 为 $\omega(p) = \omega(a_1) + \cdots + \omega(a_n)$. 集积过程要改变乘积的权. 我们在这里定义类似于集积过程的括积过程，它不改变权. 这时如果 u, v 和 (u, v) 都是基本换位子，则我们把 $\cdots uv \cdots$ 换成 $\cdots (u, v) \cdots$，而不象集积过程那样换成 $\cdots vu(u, v) \cdots$.

定理 11.2.1. 由生成元素 $x_1, \cdots, x_r$ 组成的权 n 的基本乘积数是 r^n.

证明. 对于每个 $k=1,2,\cdots$, 我们定义权 n 的全体乘积 $a_1a_2\cdots a_t$（这些 a 都是基本换位子）的族 $P_k=P_k^{(n)}$,这些乘积有形状

$$c_1^{e_1}c_2^{e_2}\cdots c_k^{e_k}c_{i_1}\cdots c_{i_s}, \tag{11.2.2}$$

这里 $e_i\geqslant 0$, $i_1>k$, $i_2,\cdots,i_s\geqslant k$, 而且对于每个换位子 $c_{i_j}=(c_u,c_v)$, 都有 c_v 在 c_k 之前. 因而 P_k 可以看作这样的字的族,在其中 $c_1,\cdots,c_{k-1}$ 已经集积而 c_k 则否. 我们把 P_k 中的乘积数记做 $|P_k|$. 显然 P_1 是 n 个生成元素的全体乘积的族,所以 $|P_1|=r^n$. 但是我们可以在 P_k 和 P_{k+1} 的元素之间建立一一对应. 事实上,如果 $c_1^{e_1}\cdots c_k^{e_k}c_{i_1}\cdots c_{i_s}$ 是 P_k 的元素,则 c_{i_1} 在 c_k 之后,因而即使在未集积的部分可以有一串 c_k, 但是紧接这一串之左必定有一个 c_y, $y>k$. 对于每一串

$$c_yc_k\cdots c_kc_w, \qquad y>k, \qquad w>k,$$

我们使用括积法 $(((c_y,c_k),c_k)\cdots,c_k)c_w$. 于是因为当 $c_y=(c_u,c_v)$ 时有 $k>v$,所以导入的新换位子是基本的而且后于 c_k. 这就给出 P_{k+1} 的唯一元素. 反之, 如果在 P_{k+1} 的元素中除去了所有包含 c_k 的括弧, 我们就得出 P_k 的唯一元素. 因此 $|P_k|=|P_{k+1}|$,因而对于每个 k 都有 $|P_k|=|P_1|=r^n$. 然而当 k 足够大时, P_k 将由权 n 的全体基本乘积组成. 这就证明了定理.

我们可以利用定理 11.2.1 来求出权 n 的基本换位子的个数,甚至可以求出这样的基本换位子的个数,它对于每个生成元素的权是特殊化了的. 我们用这样的规则来定义权 $\omega_i(c)$, $i=1,\cdots,r$: $\omega_i(x_i)=1$, $\omega_i(x_j)=0$ 对于 $i\neq j$,而且按递归法则定义 $\omega_i[(c_u,c_v)]=\omega_i(c_u)+\omega_i(c_v)$. 设 $M_r(n)$ 是 r 个生成元素 $x_1,x_2\cdots,x_r$[1] 的权 n 的换位子的个数, 再设

1) 原书有错.——译者

$M(n_1, n_2, \cdots, n_r)$ 是使 $\omega_i(c) = n_i, i = 1, \cdots, r$ 具有 $n = n_1 + n_2 + \cdots + n_r$ 的换位子 c 的个数。

定理 11.2.2 (维特定理).

$$M_r(n) = \frac{1}{n} \sum_{d \mid n} \mu(d) r^{n/d}. \tag{11.2.3}$$

$$M(n_1, n_2, \cdots, n_r) = \frac{1}{n} \sum_{d \mid n_i} \mu(d) \left(\frac{n}{d}\right)! \Big/ \left(\frac{n_1}{d}\right)! \cdots \left(\frac{n_r}{d}\right)! \tag{11.2.4}$$

这里 $\mu(m)$ 是对正整数定义的茂比乌斯函数，其规则是

$$\mu(1) = +1,$$

而对于 $n = p_1^{e_1} \cdots p_s^{e_s}$; $p_1, \cdots, p_s$ 是不同的素数，那么当有任何 $e_i > 1$ 时，$\mu(n) = 0$，而且 $\mu(p_1 p_2 \cdots p_s) = (-1)^s$.

证明. 根据定理 11.2.1，基本乘积的个数是 r^n. 这导向关于一个变数 z 的幂级数的恒等式:

$$\frac{1}{1 - rz} = \prod_{n=1}^{\infty} (1 - z^n)^{-M_r(n)}. \tag{11.2.5}$$

括积过程保持权 ω_i, $i = 1, \cdots, r$ 不变. 因而以生成元素 $x_1, \cdots, x_r$ 表出的、具有权 $\omega_i(W) = n_i$ 的字 W 的个数就等于

$$\frac{n!}{n_1! \cdots n_r!}.$$

这导向 r 个变数 $z_1, \cdots, z_r$ 的恒等式

$$\frac{1}{1 - z_1 - \cdots - z_r} = \prod_{n_1, \cdots, n_r = 0}^{\infty} (1 - z_1^{n_1} \cdots z_r^{n_2})^{-M(n_1, \cdots, n_r)}. \tag{11.2.6}$$

维特(Witt[2])从这两个恒等式出发取对数，再应用茂比乌斯反演求得了定理中的公式. 我们将在这里利用迈尔-文德利(Meier-Wunderli[1]) 的一个稍有不同的结果，我们沿着类似于证明定理 11.2.1 的线索来证明它，从而得出维特公式.

我们把字 $a_1\cdots a_n$ 叫做圈状的，假如认为 a_1 在 a_n 之后，而且 $a_1a_2\cdots a_n$，$a_2\cdots a_na_1$，$\cdots$，$a_na_1\cdots a_{n-1}$ 看作是相同的字．长度 n 的圈状字 C 可能由重复 d 个字母的节段 n/d 次而得到，这里 d 是 n 的某个约数．在这种情形下我们说 C 有周期 d．每个圈状字对应于唯一的最小周期，而且这个最小周期 d 对应于唯一的长度 d 的圈状字．

引理 11.2.1. 在权 n 的基本换位子和长度与周期都是 n 的圈状字之间存在一一对应．这可以由圈状字的适当的括积给出．

证明. 设 $a_1a_2\cdots a_n$ 是长度 n 的圈状字．权 n 的圈状字组成一族 $C_k^n=C_k$，假如它们有形状 $c_{i_1}c_{i_2}\cdots c_{i_n}$，这里这些 c 都是基本换位子，而且对于任何换位子 $c_{i_j}=c_w$，当 $c_w=(c_u, c_v)$时，就有 $v<k$，又或者(1) $i_1=i_2=\cdots=i_s$（包括 $s=1$ 的情形），或者（2）$i_1,\cdots,i_s\geqslant k$ 而某个 $i_j>k$．如果（1)成立，则按定义这字也属于 C_{k+1}．如果（2）成立，我们取每一个下列形状的圈状字序列（要是存在的话）：

$$c_w, c_k, \cdots, c_k, c_t, \quad w>k, \quad t>k,$$

而且括积成：

$$((\cdots((c_w, c_k), \cdots, c_k)c_t,$$

就得到 C_{k+1} 的唯一的圈状字．从 C_{k+1} 的字除去了包含 c_k 的括弧，我们得到 C_k 的唯一的字．因此在 C_1的字和任意 k 的 C_k 的字之间存在一一对应．如果 k 足够大，换位子 c_k 的权大于 n，因而（2）不能成立．因此括积过程最后要终止而且（1）成立．这时我们的字或者是权 n 的基本换位子，或者是 $s=n/d$ 个相同的权 d 的基本换位子的序列．我们从 C_k 到 C_{k+1} 的一步括积包括一个 c_w 和若干个 c_k．因此，每一步这种括积只在一个周期内部进行，因而恰好可以在每隔一个周期内重复．因此在字内的周期数在每一步都是相同的．于是

括积全部长度 n 的圈状字产生权 n 的全体基本换位子，而且对于 $d|n$，全体权 d 的基本换位子等同地重复 n/d 次，因为当 k 足够大时它们是 C_k 的元素．这就证明了引理，甚至还要多些．

到底有多少个长度和周期都是 n 的圈状字？长度 n 和周期 d $(d|n)$ 的字产生恰好 d 个长度 n 的普通字：

$$
\begin{array}{l}
a_1\cdots a_d a_1\cdots a_d\cdots a_1\cdots a_d \\
a_2\cdots a_d a_1\cdots a_1\cdots a_d a_1 \\
\cdots\cdots\cdots\cdots\cdots\cdots \\
a_d a_1\cdots a_d\cdots a_1\cdots a_{d-1}.
\end{array}
$$

因而

$$r^n = \sum_{d|n} dM_r(d),$$

因为长度和周期都是 d 的圈状字的个数是 $M_r(d)$，而且 r^n 个普通字中的每一个都对应于唯一的周期 d．从

$$r^n = \sum_{d|n} dM_r(d) \tag{11.2.7}$$

可以得出 $M_r(n)$，因为茂比乌斯反演公式[1] 指出，如果

$$f(n) = \sum_{d|n} g(d), \tag{11.2.8}$$

则

$$g(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) f(d). \tag{11.2.9}$$

因此

$$nM_r(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) r^d,$$

即

$$M_r(n) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) r^d, \tag{11.2.10}$$

1) 参看 Hardy and Wright [1]，第 235 页．

这就是维特公式.

使 $\omega_i(W)=n_i$, $n_1+\cdots+n_r=n$ 的普通字 W 的个数等于

$$\frac{n!}{n_1!\cdots n_r!}.$$

这导出公式

$$\frac{n!}{n_1!\cdots n_r!}=\sum_{d\mid n_1,\cdots,n_r} dM\left(\frac{n_1}{d},\frac{n_2}{d},\cdots,\frac{n_r}{d}\right). \quad (11.2.11)$$

这里 d 遍历 $(n_1,\cdots,n_r)=n_0$ 的约数. 应用茂比乌斯反演,我们得出

$$M(n_1,n_2,\cdots,n_r)=\frac{1}{n}\sum_{d\mid n_1,\cdots,n_r}\mu(d)\frac{\left(\frac{n}{d}\right)!}{\left(\frac{n_1}{d}\right)!\cdots\left(\frac{n_r}{d}\right)!}, \quad (11.2.12)$$

这是第二个维特公式.

考虑具有 r 个生成元素 $x_1, x_2, \cdots, x_r$ 的整系数的自由结合环 R. m 次元素在加法下组成自由阿贝尔群 R_m,它的基底由 r^m 个乘积 $x_{i_1}\cdots x_{i_m}$ 组成. 在环中我们用下列规则定义换位子 $[u,v]$

$$[u,v]=uv-vu. \quad (11.2.13)$$

括积运算的一般性质对于环换位子也象群换位子一样地成立. 我们要来证明在群和环的换位子之间存在一个极为密切的关系,这最初由马格努斯 (Magnus[1]) 确立.

定理 11.2.3. m 次的基本乘积组成加法群 R_m 的基底.

推论 11.2.1. m 次的基本乘积线性无关.

证明. 因为根据定理 11.2.1, m 次的基本乘积的个数是 r^m, 这正是 R_m 的基元素的个数, 因此只要证明 R_m 的每个元素都能表成基本乘积的整系数的线性组合. 因为 $P_1^{(m)}=P_1$ 是

由 r^m 个乘积 $x_{i_1}\cdots x_{i_m}$ 组成的基底，而且当 k 足够大时 P_k 由基本乘积组成，所以只要把 P_k 的元素表成 P_{k+1} 的元素的整系数的线性组合. 为此需要一个恒等式. 为了简化记号，在有 s 个 v 时，记：

$$[\cdots[u, v], v\cdots], v] = [u, \overbrace{v, \cdots, v}^{s}] = [{}^s u, v^s].$$

所要的恒等式是

$$uv^s = v^s u + \sum_{j=1}^{s} \binom{s}{j} v^{s-j}[{}^j u, v^j]. \qquad (11.2.14)$$

当 $s = 1$ 时这简化成

$$uv = vu + [u, v].$$

我们利用恒等式

$$[{}^j u, v^j]v = [{}^{j+1}u, v^{j+1}] + v[{}^j u, v^j]. \qquad (11.2.15)$$

然后就可以对 s 施行归纳法来证明 (11.2.14). 这只要在 (11.2.14) 两边之右乘上 v，用 (11.2.15) 代入再归并同类项.

如果 P_k 的元素包含子序列 $\cdots uc_k\cdots c_k w\cdots u$, $w \neq c_k$, u 后于 c_k，而且一共有 s 个 c_k，我们以 $u = n$, $v = c_k$ 而应用 (11.2.14). 得到的乘积或者属于 P_{k+1}，或者还属于 P_k，但是具有较少 c_k 或具有更接近第一个字母的 c_k. 重复应用(11.2.14)，最终将把 P_k 的元素表成 P_{k+1} 的元素的整系数的线性组合. 这就证明了定理.

现在我们把单位元素 1 添加到环 R，并把有理整数看做零次元素而且用 R_0 表示它们的集合. 这个环 R 对由 $n+1$ 或更高次的项生成的双边理想取模，得到的商环记做 $\bar{R}$. 那么

$$\bar{R} = R_0 + R_1 + \cdots + R_n. \qquad (11.2.16)$$

在 $\bar{R}$ 中，带 1 的元素 $1 + z$, $z \in R_1 + \cdots + R_n$, 组成群 G，这是因为从 $z^{n+1} = 0$ 可以得出

$$(1 + z)^{-1} = 1 - z + z^2 + \cdots + (-1)^n z^n. \qquad (11.2.17)$$

如果 $1+z=1+u_m+u_{m+1}+\cdots+u_n$，这里 $u_j\in R_j$ 对于 $j=m,\cdots,n$，而且 $u_m\neq 0$，则我们说 u_m 是 $1+z$ 的首项[1]。1 的首项是 0。

引理 11.2.2. 设 u 和 $v\neq 1$ 是 G 的分别具有 s 和 t 次的首项 u_s 和 v_t 的元素. 元素 u^{-1} 和 v^{-1} 的首项是 $-u_s$ 和 $-v_t$. 如果 $s<t$，则 uv 的首项是 u_s. 如果 $t<s$，则 uv 的首项是 v_t. 如果 $t=s$ 而且 $u_s+v_t\neq 0$，则 uv 的首项是 u_s+v_t. 如果环换位子 $[u_r, v_s]$ 不是零，则它是群换位子 (u, v) 的首项.

证明. 设 $u=1+a$，$v=1+b$，$u^{-1}=1+a'$，$v^{-1}=1+b'$，那么

$$a+a'+aa'=0,\quad aa'=a'a,$$
$$b+b'+bb'=0,\quad bb'=b'b,$$
$$a=u_s+\cdots+u_n,\quad b=v_t+\cdots+v_n,$$
$$uv=1+a+b+ab.$$

从这些关系我们立刻得到引理中关于 u^{-1}，v^{-1} 和 uv 的首项的结论. 利用这些关系我们得出

$$\begin{aligned}(u,v)&=u^{-1}v^{-1}uv\\&=(1+a')(1+b')(1+a)(1+b)\\&=1+ab-ba+aa'b-bb'a+b'ab\\&\quad+a'b'a+a'b'ab,\end{aligned}$$

因而

$$(u, v)=1+[u_s, v_t]+\text{更高次项},\qquad(11.2.18)$$

这给出引理的最后一个结果.

设 $c_1, c_2, \cdots$ 是由元素 $y_1,\cdots,y_r$ 生成的自由群 F 内的基本换位子序列，又 $d_1, d_2, \cdots$ 是把 $y_1,\cdots,y_r$ 换成 $x_1,\cdots,x_r$ 而得到的环 R 中的环换位子. 再设 c_t 是权 n 的最后一个

---

1) 在前面采取的顺序的意义下.——俄译本编者注

换位子. 那么在这些 c 和 $\bar{R}$ 中的 d 之间存在由下列引理给出的对应.

引理 11.2.3. 如果在从 F 到 G 上的映射 $y_i \to 1+x_i$, $i=1,\cdots,r$ 下有 $c_i \to g_i \in G$, $i=1,\cdots,t$, 则 g_i 的首项是 d_i.

证明. 因为 $y_i \to 1+x_i$, $i=1,\cdots,r$, 所以 $g_i = 1+x_i$ 的首项是 x_i 对于 $i=1,\cdots,r$. 我们使用归纳法. 如果 $c_w=(c_u, c_v)$, $w \leqslant t$, 则根据归纳假设, g_u 的首项是 d_u, g_v 的首项是 d_v. 因此根据引理 11.2.2, (g_u, g_v) 的首项是 $[d_u, d_v]$, 假如后者不是零的话;而作为基本换位子,根据定理 11.2.3 的推论得出它确实不是零. 因此 $g_w=(g_u, g_v)$ 的首项正如引理所断定的是 $[d_u, d_v]=d_w$.

定理 11.2.4 (基底定理)[1]. 如果 F 是具有生成元素 $y_1,\cdots,y_r$ 的自由群,又如果在基本换位子序列中, $c_1,\cdots,c_t$ 是权 $1,2,\cdots,n$ 的全体换位子,则 F 的任意元素有唯一的表达式

$$f = c_1^{e_1}c_2^{e_2}\cdots c_t^{e_t} \pmod{F_{n+1}}. \qquad (11.2.19)$$

权 n 的基本换位子组成自由阿贝尔群 F_n/F_{n+1} 的基底.

证明. 我们先证明第二个论断. 假定 $c_s,\cdots,c_t$ 是权 n 的基本换位子. 根据引理 11.2.3, 如果取由

$$y_i \to 1+x_i = g_i, \quad i=1,\cdots,r \qquad (11.2.20)$$

决定的从 F 到 G 的映射, 则 $c_s,\cdots,c_t$ 的首项是对应的环换位子 $d_s,\cdots,d_t$,它们是 n 次的环基本换位子. 根据定理 11.2.2 的推论, $d_s,\cdots,d_t$ 是线性无关的,又根据引理 11.2.2, $c_s^{e_s}\cdots c_t^{e_t}$ 的首项是 $e_sd_s+\cdots+e_td_t$,因而除非 $e_s=\cdots=e_t=0$,它不会是零. 因此 $c_s,\cdots,c_t$ 是 F_n/F_{n+1} 的无关元素, 因而它们组成基底, 这是因为我们从 (11.1.4) 已经知道 F_n/F_{n+1} 的每个元素都能用 $c_s,\cdots,c_t$ 来表出. 根据 (11.1.4), f 至少有

---

1) 参看 M. Hall [6].

一个 (11.2.19) 形状的表达式. 我们必须证明它的唯一性. 事实上,如果有

$$c_1^{e_1}\cdots c_t^{e_t}\equiv c_1^{h_1}\cdots c_t^{h_t}\pmod{F_{n+1}}, \qquad (11.2.21)$$

这里 $h_i=e_i$, $i=1,\cdots,j-1$, 但是当 c_j 的权是 k 时有 $h_j\neq e_j$,则就将导出权 k 的基本换位子取模 F_{k+1} 的一个相关式. 然而这不可能成立,因而表达式 (11.2.19) 是唯一的. 这就完成了证明.

第十二章　p群理论;正则p群

12.1. 初步结果

在第四章和第十章里得到过有限p群P的某些初步性质. 我们列举如下:

1) P有大于单位元素群的中心Z(定理 4.3.1).

2) P的真子群不是自己的正规化子(定理 4.2.1).

3) 如果P的阶是p^n,则每个极大子群M的阶都是p^{n-1}而且都是正规的(定理 4.3.2).

4) P的任何p阶的正规子群都包含在P的中心内(定理 4.3.4).

5) P是超可解的(定理 10.3.4 和定理 10.2.4).

6) P是幂零的(定理 10.3.4).

12.2. 伯恩赛德基底定理. p群的自同构

设P是p^n阶的. 它的全体极大子群的交集是特征子群D,它是P的弗拉梯尼子群. 于是在同态$P \to P/D$下,生成P的元素映射成生成P/D的元素. 逆命题也成立. 这成为伯恩赛德基底定理的内容.

定理 12.2.1(**伯恩赛德基底定理**). 设D是p群P的极大子群的交集. 商群$P/D = A$是初等阿贝尔群. 如果A的阶是p^r,则生成P的每一组元素$z_1, \cdots, z_s$包含也生成P的r个元素的子组$x_1, \cdots, x_r$. 在映射$P \to A$下元素$x_1, \cdots, x_r$

映成 A 的基底 $a_1, \cdots, a_r$. 反之，P 的任何一组在 $P \to A$ 下映成 A 的生成组的 r 个元素一定生成 P.

证明. 如果M是P的极大子群，则M有指数 p 而且是正规的. 因而P/M 是 p 阶循环群. 因此 P 的每个元素的 p 次方幂和每个换位子都包含在M内. 因此全体极大子群的交集 D 包含每个 p 次方幂和每个换位子. 如果 A 的阶是 p^r，则 A 的每个基底包含 r 个元素 $a_1, \cdots, a_r$. 设 $b_1, \cdots, b_s$ 是生成 A 的元素，我们可以从其中删去等于 1 的 b 和属于由 $b_1, \cdots, b_{i-1}$ 生成的子群的 b_i 而得出 A 的基底. 因此 $s \geqslant r$ 而且 $b_1, \cdots, b_s$ 包含一个子集是 A 的基底.

现在假定 $z_1, \cdots, z_s$ 生成 P. 在映射 $P \to P/D$ 下，设 $z_i \to b_i, i = 1, \cdots, s$. 那么 $b_1, \cdots, b_s$ 生成 A，因而包含子集 $a_1, \cdots, a_r$ 是 A 的基底. 设 $x_1, \cdots, x_r$ 是映成 $a_1, \cdots, a_r$ 的 $z_1, \cdots, z_s$ 的子集. 只要我们能证明 P 的任何一组映成 A 的基底 $a_1, \cdots, a_r$ 的元素 $x_1, \cdots, x_r$ 生成 P，定理就证明了. 设 $H = \{x_1, \cdots, x_r\}$. 如果 $H \neq P$，则 H 包含在 P 的某个极大子群 M 内. 于是在 $P \to P/D = A$ 下就有 $H \to HD/D \subseteq M/D = B$，这里 B 是 A 的 p^{r-1} 阶子群. 这将与 $H = \{x_1, \cdots, x_r\} \to \{a_1, \cdots, a_r\} = A$ 矛盾. 因此 $H = P$，即 $x_1, \cdots, x_r$ 生成 P.

作为这个定理的应用，我们可以得到关于 P 的自同构群 $A(P)$ 的某些知识. 我们可以用

$$\theta(p^r) = (p^r - 1)(p^r - p)\cdots(p^r - p^{r-1})$$

种方式选取 P/D 的基底 $a_1, \cdots, a_r$. 事实上，a_1 可以取不是单位元素的 $p^r - 1$ 个元素的任何一个，而在取定了 $a_1, \cdots, a_i$ 以后，a_{i+1} 可以取不在由 $a_1, \cdots, a_i$ 生成的子群中的 $p^r - p^i$ 个元素的任何一个. 因而 A 的基底有 $\theta(p^r)$ 种选择，而且从固定基底 $a_1, \cdots, a_r$ 到任何基底 $b_1, \cdots, b_r$ 的每个映射产生 A 的一个自同构. 又因为 A 的每个自同构必须把 $a_1, \cdots, a_r$ 映

成一个基底，所以恰好有A的$\theta(p^r)$个自同构.

恰好存在生成P的$p^{r(n-r)}\theta(p^r)$个有序集合$X=(x_1,\cdots,x_r)$，因为在从X到A的基底上的映射$x_i\to a_i$，$i=1,\cdots,r$下，A的基底有$\theta(p^r)$种选择，而且对于单个a_i，D的映成a_i的傍系中的p^{n-r}个元素的任何一个都可以取做x_i. P的每个自同构把集合X映成另一个这种集合.因此P的自同构群$A(P)$可以看做这些X上的置换群. 然而$A(P)$是(正则地作用于这些X的，因为不变某个X的自同构将不变这些x的每个乘积，因而不变整个群，即是恒同自同构. 因此当k是$A(P)$的阶时，这些X在各由k个X组成的每个传递组内彼此变换.因此$p^{r(n-r)}\theta(p^r)=kt$. 这里数t可以解释成由r个元素生成P的本质上不同的方式的个数. 两个集合$X=(x_1,\cdots,x_r)$和$Y=(y_1,\cdots,y_r)$说成是以本质上相同的方式生成P，假如每个关系$w(x_1,\cdots,x_r)=1$导出$w(y_1,\cdots,y_r)=1$而且反之亦然.

同理，设$A_1(P)$是保持A/D的每个元素都不变的$A(P)$的正规子群. 这些自同构正则地变换$p^{r(n-r)}$个生成组$X=(x_1,\cdots,x_r)$，它们在同态$P\to P/D=A$下被映成A的同一个基底$a_1,\cdots,a_r$. 因而$A_1(P)$的阶整除$p^{r(n-r)}$. 由 P. 赫尔(P. Hall[2])得到的这些结果我们写成一个定理.

定理 12.2.2. 如果P是p^n阶的p群，D是P的极大子群的交集，而且$[P:D]=p^r$，则P的自同构群$A(P)$的阶整除$p^{r(n-r)}\theta(p^r)$. 保持P/D的每个元素不变的自同构群$A_1(P)$的阶是$p^{r(n-r)}$的约数.

12.3. 集积公式

设G是由元素$a_1,a_2,\cdots,a_r$生成的群. 我们将导出用

$a_1, \cdots, a_r$ 的高次换位子表出 $(a_1a_2\cdots a_r)^n$ 的公式. 我们不妨取 G 为由 $a_1, \cdots, a_r$ 生成的自由群, 因为这公式在由 r 个元素生成的任何群里自然也成立.

我们重复一下在 § 11.1 里给出的基本换位子的定义, 只是要把顺序关系说得更清楚一些.

1) $a_1, \cdots, a_r$ 是权 1 的换位子, 而且以下列规则排成全序: $a_1 < a_2 < \cdots < a_r$.

2) 如果权小于 n 的基本换位子已经定义而且排成全序, 则 (x, y) 是权 n 的基本换位子, 必要而且只要:

(a) x 和 y 是基本换位子而且 $\omega(x) + \omega(y) = n$.

(b) $x > y$.

(c) 如果 $x = (u, v)$, 则 $y \geqslant v$.

3) 权 n 的换位子在权小于 n 的换位子之后, 而对于同是权 n 的换位子 (x_1, y_1) 和 (x_2, y_2), 当 $y_1 < y_2$, 或 $y_1 = y_2$ 而 $x_1 < x_2$ 时, 有 $(x_1, y_1) < (x_2, y_2)$.

考虑

$$(a_1a_2\cdots a_r)^n = a_1(1)a_2(1)\cdots a_r(1)a_1(2)\cdots a_r(2)\cdots a_r(n). \tag{12.3.1}$$

这里我们把各个生成元素 a_i 从左到右编号成 $a_i(1)$, $a_i(2)$, $\cdots$, $a_i(n)$, 以便在公式中分出每一个字母. 因为根据换位子的定义, $SR = RS(S, R)$, 我们可以把 (12.3.1) 左边换成别的等于它的式子, 在其中一对相继的元素 SR 换成了 $RS(S,R)$. 这种代换使 R 在式子中更接近左端而且导出了一个换位子 (S, R). 经过一系列这种代换, 我们可以移动任何字母到我们希望的接近于左端的任何位置. 我们以下列方式来变更 (12.3.1). 我们先移动 $a_1(2)$ 到左边直到它在 $a_1(1)$ 右边一个位置, 然后移动 $a_1(3)$ 到左边直到它在 $a_1(2)$ 右边一个位置, 这样继续下去, 直到我们集积了全体 a_1, 在左边开端的位置.

这就完成了集积过程的第一步. 其次我们集积 a_2 到紧接这些 a_1 之右的位置.

让我们更清楚地来描述集积过程. 在第 i 步终了我们有

$$(a_1a_2\cdots a_r)^n = c_1^{e_1}c_2^{e_2}\cdots c_i^{e_i}R_1R_2\cdots R_t, \qquad (12.3.2)$$

这里 $c_1, c_2, \cdots, c_i$ 是前 i 个基本换位子，而 $R_1, \cdots, R_t$ 是后于 c_i 的基本换位子. 如果在 $R_1, \cdots, R_t$ 中间等于 c_{i+1} 的依次是 $R_{j_1}, R_{j_2}, \cdots, R_{j_s}$,我们先移动 R_{j_1} 到紧接 $c_i^{e_i}$ 之右,然后移动 $R_{j_2}, R_{j_3}, \cdots$,最后是 R_{j_s},因而记 $e_{i+1}=s$ 就使(12.3.2)变成

$$(a_1a_2\cdots a_r)^n = c_1^{e_1}c_2^{e_2}\cdots c_{i+1}^{e_{i+1}}R_1^*\cdots R_k^*, \qquad (12.3.3)$$

这是第 $i+1$ 步. 在(12.3.2)中我们说 $c_1^{e_1}\cdots c_i^{e_i}$ 是集积的部分,而 $R_1\cdots R_t$ 是未集积的部分. 但是为了确定上述过程,必须证明在任何公式中只出现基本换位子.最初的公式(12.3.1)是第零步而且只包含生成元素 a_i,它们是权 1 的基本换位子. 让我们作归纳假设: 在第 i 步时未集积的部分 $R_1\cdots R_t$ 只包含后于 c_i 的基本换位子. 在集积等于 c_{i+1} 的那些 R 时, 我们只导入这种换位子 $(c_j, c_{i+1}, \cdots, c_{i+1})$, 这里 $j\geqslant i+2$. 这种换位子是基本的,因为如果 $c_j=(c_r, c_s)$,则当 c_s 已集积时, c_j 在第 s 步出现, 因而 $s<i+1$, 于是 $c_s<c_{i+1}$, 因此(c_j, c_{i+1}) 是基本的,所以 $(c_j, c_{i+1}, \cdots, c_{i+1})$ 也是基本的.

我们在(12.3.1)里已经用号码 j 把生成元素 a_i 编号成 $a_i(j)$, $j=1, \cdots, n$. 如果权 w_1 的换位子 R 有号码 $(\lambda_1, \cdots, \lambda_{w_1})$, 权 w_2 的换位子 S 有号码$(\mu_1, \cdots, \mu_{w_2})$,则我们令$(R, S)$ 有号码$(\lambda_1, \cdots, \lambda_{w_1}, \mu_1, \cdots, \mu_{w_2})$.(12.3.3)中方次数 $e_1, \cdots, e_i, e_{i+1}$ 的计算运用这些记号来进行. 这时 $e_{i+1}=s$ 是在第 i 步时等于 c_{i+1} 的未集积的换位子的个数. 因而这是在这一步时存在的换位子 c_{i+1} 的个数 E_{i+1}. 又如果 $c_{i+1}=(c_r, c_s)$;则在集积 c_s 时会产生 c_{i+1}, 而且这个特定的 c_r 在未集积的部分

中在这个特定的 c_s 之左．因此我们还必须考虑，当 c_r 和 c_s 都在未集结部分中时，c_r 在 c_s 之左的领先条件．

在第零步时有的是权 1 的换位子（而没有别的），因而 $a_k(\lambda)$ 对于任何号码 $\lambda = 1, \cdots, n$ 都存在．其次，在第零步时，对于 $k \geqslant s$，当 $\lambda < \mu$ 时，$a_k(\lambda)$ 在 $a_s(\mu)$ 之左，而对于 $k < s$，则当 $\lambda \leqslant \mu$ 时，$a_k(\lambda)$ 在 $a_s(\mu)$ 之左．总之，在第零步时，我们有下列用号码表出的关于未集结部分的存在和领先条件：

$E_k^0[a_k(\lambda)]$，如果 λ 存在(空集条件)．

$P_{rs}^0[a_r(\lambda)$ 在 $a_s(\mu)$ 之左$]$：当 $r \geqslant s$ 时，$\lambda < \mu$

当 $r < s$ 时，$\lambda \leqslant \mu$．

设 $\lambda_1, \cdots, \lambda_m$ 是一组整数，我们考虑下列类型的条件：$\lambda_t < \lambda_u$，$\lambda_t \leqslant \lambda_u$．我们把这种条件的逻辑和以及逻辑乘积叫做条件 (L)．我们将证明在第 i 步具有号码 $(\lambda_1, \cdots, \lambda_m)$ 的换位子 c_k 的存在条件 E_k^i 是关于 $\lambda_1, \cdots, \lambda_m$ 的条件 (L)，而在第 i 步的未集积部分中换位子 c_r 在换位子 c_s 之左的领先条件 P_{rs}^i 是关于 $\lambda_1, \cdots, \lambda_m, \mu_1, \cdots, \mu_q$ 的条件 (L)，这里 $(\lambda_1, \cdots, \lambda_m)$ 是 c_r 的号码，$(\mu_1, \cdots, \mu_q)$ 是 c_s 的号码．我们已经看到，在第零步时，存在条件和领先条件确实是条件 (L)．我们对步数施行归纳法来证明这结论成立．为了证明这在第 $i+1$ 步时成立，我们来比较 (12.3.2) 和 (12.3.3)．当 $R_{j_1} = R_{j_2} = \cdots = R_{j_s} = c_{i+1}$ 时，我们先集积 R_{j_1}，然后 $R_{j_2}, \cdots$，最后 R_{j_s}．每一步集积都是进行代换 $SR = RS(S, R)$．这时在第 i 步存在的与 c_{i+1} 不同的换位子在第 $i+1$ 步也存在而且顺序不变．因而对于这种换位子有 $E_k^{i+1} = E_k^i$ 和 $P_{rs}^{i+1} = P_{rs}^i$．因此我们只要考虑在第 $i+1$ 步时出现换位子 c_k 的存在条件和出现 c_r，c_s 中一个或两个的领先条件．在这一步出现的换位子有形状 $c_k = (c_j, R_{u_1}, \cdots, R_{u_m})$，得出它是由于把 R_{u_1} 移过 c_j，然后把 R_{u_2} 移过这个换位子，等等，直到把 R_{u_m} 移过 $(c_j,$

$R_{u_1}, \cdots, R_{u_{m-1}}$). 这时所有 $R_{u_1}, \cdots, R_{u_m}$ 都等于 c_{i+1}. 这里 E_k^{i+1} 是在 i 步时 $c_j, R_{u_1}, \cdots, R_{u_m}$ 的存在条件和在第 i 步时 $c_j, R_{u_1}, \cdots, R_{u_m}$ 就以这个次序领先的条件的逻辑乘积. 因而 E_k^{i+1} 是关于 c_k 的号码的条件 (L). 在第 $i+1$ 步集积时,在 $SR = RS(S, R)$ 中出现紧接在 S 之右而在 S 后的所有换位子之左的换位子 (S, R). 我们必须找出使 $c_r = c_j$, 或 $(c_{j_1}, R_{u_1}, \cdots, R_{u_m})$ 以及 $c_s = c_{j_2}$ 或 $(c_{j_2}, R_{v_1}, \cdots, R_{v_w})$ 的领先条件 P_{rs}^{i+1}. 这时当 $c_{j_1} \neq c_{j_2}$ 时有 $P_{rs}^{i+1} = P_{j_1 j_2}^{i}$. 但是如果 $c_{j_1} = c_{j_2}$,则 P_{rs}^{i+1} 取决于这些 R. 假定 e 是使 $R_{u_1} = R_{v_1}, \cdots, R_{u_e} = R_{v_e}$ 的最大整数. 那么 c_r 先于 c_s, 只要 (1) $m = e$ 而且不存在 $R_{u_{e+1}}$ (这时 c_s 是 c_r 的换位子), 或 (2) $R_{u_{e+1}}$ 先于 $R_{v_{e+1}}$. 于是 P_{rs}^{i+1} 是领先条件[1] 的逻辑和, 因而也就是关于 c_r 和 c_s 的号码的条件 (L) 合起来.

引理 12.3.1. 满足已知条件 (L) 的数组 $\lambda_1, \cdots, \lambda_m$ $(1 \leqslant \lambda_i \leqslant n)$ 的个数是 n 的整值多项式: $b_1 n + b_2 n^{(2)} + \cdots + b_m n^{(m)}$, 这里 $n^{(i)} = n(n-1)\cdots(n-i+1)/i!$,而 b_i 是由条件 (L) 决定但是不依赖于 n 的整数.

证明. 我们把指标 $1, \cdots, m$ 分成互不相交的集合 $S_1, S_2, \cdots, S_t$. 取 t 个数 $v_1 < v_2 < \cdots < v_t \leqslant n$. 如果在某个组 $\lambda_1, \cdots, \lambda_m$ 中有 $\lambda_j = v_i$ 对于 $j \in S_i$, 则就决定了 λ_i 按大小排的顺序. 对于 λ_i 的任何可能的选择, 存在这种类型的唯一顺序[2], 而且这些 v 有 $n^{(t)}$种选择,这就是在 n 件东西中每次取 t 件的组合数.对于数 λ_i 的适当的顺序[3],或者所有数组 $\lambda_1, \cdots, \lambda_m$ 都满足条件 (L), 或者任何一组都不满足. 因此满足已知条

1) 对于 $i+1$ 之前的各步.——俄译者注

2) 对于适当的剖分 $S_1, S_2, \cdots, S_t$ 和数 $v_1 < v_2 < \cdots < v_t \leqslant n$.
——俄译本编者注

3) 对于固定的剖分 $S_1, S_2, \cdots, S_t$ 和所有可能的选择 $v_1 < v_2 < \cdots < v_t \leqslant n$.
——俄译本编者注

件 (L) 的数组 $\lambda_1, \cdots, \lambda_m$ 的个数是多项式 $b_1n + b_2n^{(2)} + \cdots + b_mn^{(m)}$，这里 b_t 是具有满足条件 (L) 的 t 个不同的值的顺序数，显然 b_t 取决于这些条件而不取决于 n.

举例说，如果 $\lambda_1, \lambda_2, \lambda_3$ 满足条件 (L) $\lambda_1 < \lambda_2$, $\lambda_3 \leqslant \lambda_2$，则满足 ($L$) 的顺序是

1) $\lambda_1 = v_1$, $\lambda_2 = \lambda_3 = v_2$, $v_1 < v_2$,

2) $\lambda_1 = \lambda_3 = v_1$, $\lambda_2 = v_2$, $v_1 < v_2$,

3) $\lambda_1 = v_1$, $\lambda_3 = v_2$, $\lambda_2 = v_3$, $v_1 < v_2 < v_3$,

4) $\lambda_3 = v_1$, $\lambda_1 = v_2$, $\lambda_2 = v_3$, $v_1 < v_2 < v_3$,

而满足条件 (L) 的数组的个数是 $2n^{(2)} + 2n^{(3)}$.

我们已经证明了 (12.3.2) 中的换位子 c_i 的方次数 e_i 是在第 $i-1$ 步的未集积部分中等于 c_i 的换位子的个数，而且这个数又是满足某些条件 (L) 的数组 $\lambda_1, \cdots, \lambda_m$ 的个数，这里 m 是 c_i 的权. 因而引理 12.3.1 提出的是关于这些方次数的结果. 我们把它写成一个定理

定理 12.3.1. 乘积 $(a_1a_2\cdots a_r)^n$ 可以表成 $(a_1a_2\cdots a_r)^n = a_1^na_2^n\cdots a_r^n c_{r+1}^{e_{r+1}}\cdots c_i^{e_i}R_1\cdots R_t$，这里 $c_{r+1}, \cdots, c_i$ 是元素 $a_1, \cdots, a_r$ 的排成顺序的基本换位子，而 $R_1, \cdots, R_t$ 是在这顺序下后于 c_i 的基本换位子. 当 $1 \leqslant j \leqslant i$ 时，方次数 e_j 有形状 $e_j = b_1n + b_2n^{(2)} + \cdots + b_mn^{(m)}$，这里 m 是 c_j 的权，而且 $b_1, \cdots, b_m$ 是不依赖于 n 而只依赖于 c_j 的非负整数. 这里

$$n^{(k)} = n(n-1)\cdots(n-k+1)/k!.$$

我们立刻可以证明当 G 是类小于 p 的 p 群时的重要推论. 集积全体权小于 p 的换位子，未集积部分简化成单位元素. 其次，当 $n = p^\alpha$ 时，所有方次数都是 p 的倍数，因为 $n^{(i)}$, $i \leqslant p-1$ 是这样的二项式系数，它的分子包含因子 n，而分母的各个因子都不大于 $p-1$.

推论 12.3.1. 如果 P 是类小于 p 的 p 群，则当 $n = p^\alpha$ 时，

$$(a_1a_2\cdots a_r)^n = a_1^na_2^n\cdots a_r^nS_1^nS_2^n\cdots S_t^n,$$

这里 $S_1, S_2, \cdots, S_t$ 属于由 $a_1, a_2, \cdots, a_r$ 生成的群的换位子子群.

12.4. 正则 p 群

我们把 p 群 P 叫做正则的，假如对于任何两个元素 a 和 b 以及任何 $n = p^\alpha$,都有

$$(ab)^n = a^nb^nS_1^n\cdots S_t^n, \tag{12.4.1}$$

这里 $S_1, \cdots, S_t$ 是由 a 和 b 生成的群的换位子子群（即导出群)的元素. 从定义和定理 12.3.1 的推论立刻得出:

1）类小于 p 的每个 p 群是正则的.

2）阶不大于 p^p 的每个 p 群是正则的.

3）如果 P 的每个由两个元素生成的子群是正则的,则 P 也是正则的.

4）正则 p 群的每个子群和商群都是正则的.

对于每个 p 都存在阶为 p^{p+1} 的非正则 p 群,那就是 p^2 个文字上的对称群 S_{p^2} 的西罗子群 $S^{(p)}$. 这个群由两个 p 阶元素生成,但是它包含着 p^2 阶的元素. 将会证明这对于正则 p 群是不可能的.

定理 12.4.1. 在正则 p 群内,当 $n = p^\alpha$ 时有

$$a^nb^n = (ab)^nS_1^n = (abS_2)^n,$$

这里 S_1, S_2 在由 a 和 b 生成的群 $H(a, b)$ 的导出群 $H_2(a,b)$.

重复应用这个定理可以得出下列推论:

推论 12.4.1. 在正则 p 群内,当 $n = p^\alpha$ 时有

$$a_1^na_2^n\cdots a_r^n = (a_1a_2\cdots a_r)^nS_1^n = (a_1a_2\cdots a_rS_2)^n,$$

这里 S_1, S_2 在 $H_2(a_1\cdots a_r)$ 内.

证明. 定理和推论在阿贝尔群的情形都成立,这时 $S_1=1$,

$S_2=1$. 我们运用归纳法来证明定理对于任何子群H成立，这时假定定理和它的推论对于H的任意真子群成立. 我们注意到，如果H由$a_1, \cdots, a_r$生成，则H的导出群$H_2(a_1, \cdots, a_r)$是H的真子群. 从(12.4.1)有

$$a^n b^n=(ab)^n S_r^{-n}\cdots S_1^{-n}. \qquad (12.4.2)$$

根据归纳假设，$S_r^{-n}\cdots S_1^{-n}=S^n$，这里$S\in H_2$. 但是如果$H=H(a, b)$不是阿贝尔群，则$H_2$和$ab$生成$H$的真子群，因而根据归纳假设有$(ab)^n S^n=(abS_2)^n$. 事实上. 从伯恩赛德基底定理得出，如果$H/H_2$是循环群，则$H$是循环群. 因而当定理和推论在$H$的任何真子群内成立时，定理在$H$内成立. 定理对$a_1^n a_2^n\cdots a_r^n$应用$r-1$次，我们得出

$$a_1^n a_2^n\cdots a_r^n=(a_1a_2\cdots a_r)^n S_1^n\cdots S_{r-1}^n,$$

这里全体$S_1, \cdots, S_{r-1}$都在H_2内. 因而对H_2应用引理就有$a_1^n\cdots a_r^n=(a_1a_2\cdots a_r)^n S^n$，再根据定理，

$$(a_1a_2\cdots a_r)^n S^n=(a_1a_2\cdots a_rS_1)^n.$$

定理 12.4.2. 有限p群P是正则的，必要而且只要对于P中的任何a和b，都有

$$a^p b^p=(ab)^p S^p, \qquad (12.4.3)$$

这里S在由a和b生成的群的导出群内.

条件(12.4.3)在正则p群内显然成立，因为它是定理12.4.1的特殊情形. 反过来我们必须证明从(12.4.3)得出

$$a^n b^n=(ab)^n S_1^n,\ n=p^\alpha,\ S_1\in H_2(a, b). \qquad (12.4.4)$$

现在来考虑关系式：

$$a_1^p a_2^p\cdots a_r^p=(a_1a_2\cdots a_r)^p S_1^p=(a_1a_2\cdots a_rS_2)^p, \quad (12.4.5)$$

这里$S_1, S_2\in H_2(a_1, \cdots, a_r)$. 当$H$是阿贝尔群时，这等式显然以$S_1=S_2=1$而成立. 如果(12.4.5)对于$H$的每个真子群都成立，则应用(12.4.3) $r-1$次，就得出

$$a_1^p a_2^p\cdots a_r^p=(a_1a_2\cdots a_r)^p u_1^p\cdots u_{r-1}^p,$$

这里 $u_1, \cdots, u_{r-1}$ 在 H_2 内. 根据归纳假设, $u_1^p \cdots u_{r-1}^p = S_1^p$. 然而 $b = a_1a_2\cdots a_r$ 和 S_1 生成H的真子群,因而

$$(a_1a_2\cdots a_r)^pS_1^p = (a_1\cdots a_rS_2)^p,$$

这就在一般情形证明了(12.4.5).

引理 12.4.1. 如果(12.4.3)成立, 则 $x^{-p}y^{-p}x^py^p = S^p$, 这里 S 属于 $\{x, y\}$ 的导出群.

证明.

$$x^py^p = (x, y)^pS_1^p,$$
$$y^px^p = (y, x)^pS_2^p,$$

因而

$$x^{-p}y^{-p}x^py^p = S_2^{-p}(y, x)^{-p}(x, y)^pS_1^p,$$

再有

$$(y, x)^{-p}(x, y)^p = (x^{-1}y^{-1}xy)^pS_3^p = (x, y)^pS_3^p,$$

所以

$$x^{-p}y^{-p}x^py^p = S_2^{-p}(x, y)^pS_3^pS_1^p = S^p.$$

由此得出,元素 $a_1^p, a_2^p, \cdots, a_r^p$ 的任何换位子是 $\{a_1,\cdots, a_r\}$ 的导出群的一个元素的 p 次方幂.

从(12.4.3)得出

$$a^{p^2}b^{p^2} = (a^pb^p)^pS_1^p = [(ab)^pS_2^p]^pS_1^p = (ab)^{p^2}S_2^{p^2}S_3^pS_1^p, \tag{12.4.6}$$

这里 S_1 属于 $\{a^p, b^p\}$ 的导出群, S_3 属于 $\{(ab)^p, S_2^p\}$ 的导出群. 根据引理, 它们是 $\{a, b\}$ 的导出群的元素的 p 次方幂, 因而

$$a^{p^2}b^{p^2} = (ab)^{p^2}S_2^{p^2}S_4^{p^2}S_5^{p^2}, \tag{12.4.7}$$

于是应用归纳法得出(12.4.4)对于 $n = p^2$ 成立. 用同样的论证而且利用引理,就可以从假设 $n = p^\alpha$ 时(12.4.4)成立来证明它在 $n = p^{\alpha+1}$ 时也成立.

定理 12.4.3. 如果 P 是正则 p 群,则当 $n = p^\alpha$ 时:

1) 从 $(a^n, b) = 1$ 得出 $(a, b)^n = 1$, 反之亦然.

2）如果 $(a^n, b)=1$，则 $(a, b^n)=1$.

3）包含元素 u 的换位子 S 的阶不超过元素 u 取模 Z 的阶，这里 Z 是 P 的中心.

4）乘积 $a_1a_2\cdots a_r$ 的阶不大于每个元素 $a_1, a_2, \cdots, a_r$ 的阶[1].

证明. 在阿贝尔群内，前三个性质显然成立，而且第四个也不难验证. 我们归纳地假设定理对于 P 的全部真子群成立，而且取 P 是非阿贝尔群.

我们应用(12.4.4)到

$$a^{-n}b^{-1}a^nb=(a^{-1})^n(b^{-1}ab)^n=(a^{-1}b^{-1}ab)^n s^n, \quad (12.4.8)$$

这里 s 属于 $K(a, b^{-1}ab)\subset H(a, b)$的导出群；这就成为

$$(a^n, b)=(a, b)^n s_1^n. \quad (12.4.9)$$

现在如果$(a^n, b)=1$，则 a 取 $H(a, b)$ 的中心 Z 为模的阶是 n 或更小，因而根据关于真子群 $K(a, b^{-1}ab)$ 的性质3而且取 $u=a$，就有 K 的每个换位子包含 a 而且它的阶最多是 n. (12.4.9) 中的元素 s_1 是 K 内的换位子的乘积，而且根据关于 K 的(4)，s_1 的阶最多是 n. 因而从 $(a^n, b)=1$ 得出(12.4.9)中有 $s_1^n=1$，所以 $(a, b)^n=1$. 反之，如果 $(a, b)^n=1$，则在 $u=(a, b)$ 的 $K=K(a, a^{-1}ab)=K(a, u)$ 中，u 取中心为模的阶最多是 n，而且每个换位子都包含 u. 因而根据关于 K 的(3)，K_2 内的任何换位子的阶最多是 n，所以根据 K_2 中的(4)，(12.4.9)中的 s_1 的阶最多是 n.

因此从 $(a, b)^n=1$ 得出 $S_1^n=1$，于是 $(a^n, b)=1$. 这就证明了关于 P 的性质(1). 于是(2)直接从(1)得出. P 中的性质(3)可以从重复应用(1)而得到. 如果 u 取 P 的中心为模的阶是 n，则当然有 $(u^n, v)=1$，因而 $(u, v)^n=1$.

1）这里和以后提到的元素 $a\in P$ 在商群 P/Z 内的阶当然是指 P 对 Z 的包含 a 的傍系的阶.——俄译本编者注

这时如果取 $x=(u,v)$,则由于 $x^n=1$,所以 $(x,y)^n=1$.

还需要证明关于 P 的性质(4). 如果 $a^n=1$, $b^n=1$,则根据(3), 包含 a 或 b 的任何换位子的阶最多是 n. 因此在(12.4.4)中, S_1 是最多有阶 n 的换位子的乘积,而且根据关于真子群 P_2 的性质(4), S_1 本身的阶最多是 n. 因此 $S_1^n=1$,所以 $(ab)^n=1$. 于是两个因子的乘积的阶不大于各个因子的阶. 重复这个结论可以推出 r 个因子的乘积的阶不大于各个因子的阶.

定理 12.4.4. 如果 $a^n=b^n$ 而且 $n=p^\alpha$, 则 $(ab^{-1})^n=1$, 反之亦然.

证明. 在 $H(a,b)$ 内,根据定理 12.4.3 中的性质(3), 任何交换者的阶不大于 n. 因此在 $1=a^nb^{-n}=(ab^{-1})^ns_1^n$ 中我们有 $s_1^n=1$, 所以 $(ab^{-1})^n=1$. 反之,设 $a^nb^{-n}=(ab^{-1})^ns_1^n$, $(ab^{-1})^n=1$ 而且 $H(a,b)=H(a,ab^{-1})$. 那么从关于元素 $u=ab^{-1}$ 的性质(3),我们得出 $s_1^n=1$,因而 $a^n=b^n$.

定理 12.4.5. 在正则 p 群 P 中,元素的 p^α 次方幂组成特征子群 $C^\alpha(P)$,阶不大于 p^α 的元素组成特征子群 $C_\alpha(P)$.

证明. 当 $n=p^\alpha$ 时,定理 12.4.1 的关系式 $a^nb^n=(abS_2)^n$ 指出,元素的 p^α 次方幂组成子群 $C^\alpha(P)$, 它必定是特征子群, 甚至还是完全不变子群. 定理 12.4.3 的性质(4)指出. 阶不大于 p^α 的元素组成一个子群,它是完全不变的.

12.5. 一些特殊 p 群. 哈密尔顿群

定理 12.5.1. 包含着指数为 p 的循环子群的 p^n 阶群有下列类型:

阿贝尔群,

$n\geqslant 1$,循环群:

1) $a^{p^n}=1$.

$n\geqslant 2$:

2) $a^{p^{n-1}}=1$, $b^p=1$, $ba=ab$.

非阿贝尔群,

p 奇数, $n\geqslant 3$:

3) $a^{p^{n-1}}=1$, $b^p=1$, $ba=a^{1+p^{n-2}}b$.

$p=2$, $n\geqslant 3$:

4) 广义四元数群.

$a^{2^{n-1}}=1$, $b^2=a^{2^{n-2}}$, $ba=a^{-1}b$.

$p=2$, $n\geqslant 3$

5) 二面体群.

$a^{2^{n-1}}=1$, $b^2=1$, $ba=a^{-1}b$.

$p=2$, $n\geqslant 4$

6) $a^{2^{n-1}}=1$, $b^2=1$, $ba=a^{1+2^{n-2}}b$.

$p=2$, $n\geqslant 4$

7) $a^{2^{n-1}}=1$, $b^2=1$, $ba=a^{-1+2^{n-2}}b$.

证明. 包含 p^{n-1} 阶元素的 p^n 阶群必定有 p^{n-1} 阶或 p^n 阶的基元素. 因此当这群是阿贝尔群时就有定理中的前两种情形.

在讨论包含 p^{n-1} 阶元素的 p^n 阶非阿贝尔群时,我们先假定 p 是奇数. 如果 $a^{p^{n-1}}=1$, 则$\{a\}$作为指数 p 的子群是正规子群,因而对于 $b\notin\{a\}$ 有 $bab^{-1}=a^r$,这里 $r\not\equiv 1\ (\mathrm{mod}\ p^{n-1})$, 因为我们考虑的不是阿贝尔群. 对 i 施行归纳法可以证明 $b^iab^{-i}=a^{r^i}$. 事实上, 对于任何 j, $(bab^{-1})^j=ba^jb^{-1}=a^{rj}$, 特别当 $j=r$ 时有 $b^2ab^{-2}=b(bab^{-1})b^{-1}=ba^rb^{-1}=a^{r^2}$. 然后可以用归纳法得出一般情形的 $b^iab^{-i}=a^{r^i}$. 由于 $b^p\in\{a\}$, 我们有 $b^pab^{-p}=a$, 因而 $r^p\equiv 1\ (\mathrm{mod}\ p^{n-1})$. 因为 p 是奇数, 我们从这个同余式得出 $r\equiv 1+kp^{n-2}(\mathrm{mod}\ p^{n-1})$, 这里 $k\not\equiv$

$0 \pmod p$，因为 $r \not\equiv 1 \pmod{p^{n-1}}$.现在取 $b_1 = b^i$，这里 i 由同余式 $ik \equiv 1 \pmod p$ 决定。于是 $r^i \equiv (1 + kp^{n-2})^i \equiv 1 + ikp^{n-2} \equiv 1 + p^{n-2} \pmod{p^{n-1}}$. 因此 $b_1 a b_1^{-1} = b^i a b^{-i} = a^{r^i} = a^{1+p^{n-2}}$. 我们记 $h = 1 + p^{n-2}$. 那么 $(a^j b_1)^2 = a^j b_1 a^j b_1^{-1} b_1^2 = a^{j(1+h)} b_1^2$，而且可以用归纳法证明 $(a^j b_1)^t = a^{jT} b^t$，这里 $T = 1 + h + \cdots + h^{t-1}$. 当 $t = p$时，我们有 $1 + h + \cdots + h^{p-1} \equiv p + p^{n-2}[1 + 2 + \cdots + (p-1)] \equiv p + p^{n-1}(p-1)/2 \equiv p \pmod{p^{n-1}}$，因为 p 是奇数。因而 $(a^j b_1)^p = a^{jp} b_1^p$. 这个关系也可以利用集积公式得出。现在 $b_1^p = a^u \in \{a\}$，这里$u = pv$，因为 b 不是 p^n 阶的，而且已知群不是循环群。如果我们令 $b_2 = a^{-v} b_1$；则 $b_2^p = (a^{-v} b_1)^p = a^{-vp} b_1^p = a^{-pv} a^{pv} = 1$，又

$$b_2 a b_2^{-1} = a^{-v} b_1 a b_1^{-1} a^v = a^{-v} a^{1+p^{n-2}} a^v = a^{1+p^{n-2}}.$$

因此 a 和 b_2 满足定理中第 3 类型 p 是奇数的非阿贝尔群的关系.

现在我们取 $p = 2$，来找出包含 2^{n-1} 阶元素的 2^n 阶非阿贝尔群。设 $a^{2^{n-1}} = 1$, $b \notin \{a\}$. 那么 $bab^{-1} = a^r$，这里 $r^2 \equiv 1 \pmod{2^{n-1}}$，$r \not\equiv 1 \pmod{2^{n-1}}$. 这给出 r 取模 2^{n-1} 的三种可能情形：$r = -1$，　$r = 1 + 2^{n-2}$，　$r = -1 + 2^{n-2}$. 再设 $b^2 = a^w \in \{a\}$. 那么因为 $b(b^2)b^{-1} = b^2$，所以 $a^{wr} = a^w$ 或 $wr \equiv w \pmod{2^{n-1}}$，这是$w$所满足的条件。当 $r = -1$ 时我们有 $-w \equiv w \pmod{2^{n-1}}$，因而 $a^w = 1$ 或 $a^w = a^{2^{n-2}}$. 总之当 $r = -1$ 时我们得出广义的四元数群或二面体群，这分别是定理中的类型 4 和 5。当 $n = 3$ 时，我们在 § 4.4 中决定过只有这些群.

现在假定 $n \geqslant 4$ 而且 $ba = a^r b$，这里 $r = 1 + 2^{n-2}$. 当 $b^2 = a^w$ 时，w所满足的条件 $wr \equiv w \pmod{2^{n-2}}$ 只不过是 $2^{n-2} w \equiv 0 \pmod{2^{n-1}}$，即$w$是偶数 $w = 2w_1$. 从同余式 $j(1 + 2^{n-3}) + w_1 \equiv 0 \pmod{2^{n-2}}$ 决定 j. 那么当 $b_1 = a^j b$ 时有 $b_1^2 =$

$a^j(ba^j)b = a^{j(2+2^{n-2})}b^2 = a^{2[j(1+2^{n-3})+w_1]} = a^{2^{n-1}}=1$. 这时$b_1a = a^{1+2^{n-2}}b_1$,因而 a 和 b_1 满足定理中类型 6 的关系. 最后, 如果 $n \geqslant 4$, $ba = a^rb$, 这里 $r = -1 + 2^{n-2}$, 则在 $b^2 = a^w$ 中 w 所满足的条件 $w \equiv rw \pmod{2^{n-1}}$ 是 $(2 + 2^{n-2})w \equiv 0 \pmod{2^{n-1}}$ 或 $w \equiv 0 \pmod{2^{n-2}}$. 因而 $b^2 = 1$ 或 $b^2 = a^{2^{n-2}}$. 如果 $b^2 = a^{2^{n-2}}$,则取 $b_1 = ab$ 后有

$$b_1^2 = a(ba)b = a(a^{-1+2^{n-2}})b^2 = a^{2^{n-2}}a^{2^{n-2}} = 1.$$

因而 a 和 b 或者 a 和 b_1 满足定理中类型 7 的关系.

利用定理 6.5.1 容易验证,定理 12.5.1 中除广义四元数群外的所有情形的关系都能决定群. 至于四元数群, 我们可以直接验证,也可以运用定理 15.3.1 来验证.

定理 12.5.2. 只包含一个 p 阶子群的 p 群或是循环群,或是广义四元数群.

证明. 设 P 是 p^n 阶的而且只包含一个 p 阶子群. 我们对 n 施行归纳法来证明 P 或是循环群, 或是广义四元数群. 当 $n = 1$ 时这是显然的. 先假定 p 是奇数. 于是根据归纳假设, 指数 p 的子群 P_1 是循环群, 因而根据定理 12.5.1, P 属于 p 是奇数的类型 1, 2 或 3 中的一个, 而在其中类型 2 和 3 包含多于一个 p 阶子群. 因此 P 是循环群. 当 $p = 2$ 时,如果 P 包含指数为 2 的循环子群 P_1,则根据定理 12.5.1, P 是 $p=2$ 的类型 1 到 7 中的一个,而在这些类型中,除循环群和广义四元数群外, 都包含多于一个的 2 阶子群. 因而 P 是循环群或广义四元数群.

还需要考虑指数为 2 的每个子群 P_1 都是广义四元数群的情形. 我们来证明这种情形不可能成立. 这时 $n \geqslant 4$. 先设 $n = 4$ 而且指数为 2 的一个子群是四元数群 Q,再设 c 是不属于 Q 的元素. Q 满足关系

$$a^4 = b^4 = 1,\ a^2 = b^2,\ ba = a^{-1}b,$$

而且 $P = Q + Qc$. 元素 c 的阶是 2 的方幂，它至少把 Q 的三个二阶子群 $\{a\}$, $\{b\}$, $\{ab\}$ 中的一个变成自己. 不失去普遍性，不妨说这是 $\{a\}$. 于是 $c^{-1}ac = a$ 或 $c^{-1}ac = a^{-1}$. 如果 $c^{-1}ac = a$，则 $\{a, c\}$ 是指数 2 的阿贝尔子群而与假设矛盾. 如果 $c^{-1}ac = a^{-1}$,则 $(cb)^{-1}a(cb) = a$，因而 $\{a, cb\}$ 是指数 2 的阿贝尔子群而与假设矛盾. 这样就排除了 $n = 4$ 的情形.

最后，假定 $n \geqslant 5$ 而且 P_1 是指数为 2 的广义四元数子群. 那么 P_1 满足下列关系: $a^{2^{n-2}} = 1$, $b^2 = a^{2^{n-3}}$, $ba = a^{-1}b$, 而且 $P = P_1 + P_1c$. 这时 $\{a\}$ 是 P_1 的唯一的 2^{n-2} 阶子群，而 P_1 的不在 $\{a\}$ 内的每个元素都是 4 阶的. 因而 $c^{-1}ac = a^r$. 而且 $c^2 = a^ib$ 或 $c^2 = a^i$. 如果 $c^2 = a^ib$，则 $c^{-2}ac^2 = a^{-1}$, 因而 $r^2 \equiv -1 \pmod{2^{n-2}}$, 这是不可能的. 如果 $c^2 = a^i$, 则 $\{a, c\}$ 是指数 2 的子群，因而根据归纳假设它是广义四元数群. 于是 $c^{-1}ac = a^{-1}$, $(cb)^{-1}a(cb) = a$, 因而 $\{cb, a\}$ 是指数为 2 的阿贝尔子群而与假设矛盾. 这就在所有情形完成了定理的证明.

定理 12.5.3. 当 $1 < m < n$ 时，只包含一个 p^m 阶子群的 p^n 阶群是循环群.

证明. 如果 $m = n - 1$，则已知群 P 是具有唯一 p^{n-1} 阶子群的 p^n 阶群，它由不在这子群内的任何元素 x 生成，因为 $\{x\}$ 不包含在这个唯一的极大子群内，所以 $\{x\} = P$, 即 P 是循环群. 这证明了 $n = 3$ 时的定理，这是定理适用的 n 的第一个值，而且也在 $m = n - 1$ 的所有情形证明了定理. 我们对 n 施行归纳法. 我们已经在 $m = n - 1$ 时证明了定理，因而可以假定 $m < n - 1$.

设 P_1 是唯一的 p^m 阶子群，再设 P_1 包含在 p^{n-1} 阶的极大子群 A 内. 因为 $1 < m < n - 1$，根据归纳假设，A 是循环

群，因而作为 A 的子群的 P_1 也是循环群．因为 $m \geqslant 2$，每个 p 阶或 p^2 阶子群包含在 p^m 阶子群内，因而包含在 P_1 内．但是 P_1 是循环群，它包含着唯一的 p 阶子群和唯一的 p^2 阶子群．因而 P 包含着唯一的 p 阶子群和唯一的 p^2 阶子群．根据定理 12.5.2，P 是循环群或广义四元数群．但是广义四元数群包含多于一个 4 阶子群．因此 P 必定是循环群．

阿贝尔群的每个子群当然是正规的．而四元数群是每个子群都是正规子群的非阿贝尔群的一个特例．我们把群 H 叫做哈密尔顿群，假如 H 不是阿贝尔群，但是它的每个子群都是正规子群．

定理 12.5.4. 哈密尔顿群是三个群的直积：四元数群，每个元素的阶都是奇数的阿贝尔群和方次数[1] 为 2 的阿贝尔群．

证明． 设 a 和 b 是哈密尔顿群 H 的两个元素．那么换位子 $c = (a, b) = (a^{-1}b^{-1}a)b = b^s = a^{-1}(b^{-1}ab) = a^r$，因为 $\{a\}$ 和 $\{b\}$ 都是正规子群．注意由此得出 c 既与 a 可交换，也与 b 可交换．根据 (10.2.1)．

$$(a^2, b) = (a, b)(a, b, a)(a, b)$$
$$= (a, b)(c, a)(a, b) = (a, b)^2,$$

同理可以用归纳法证明

$$(a^i, b) = (a, b)^i = c^i.$$

如果 a 和 b 不能交换，则 $c = a^r \neq 1$，这时取 $i = r$ 或 $i = -r$ 中的正值，那么 (a^i, b) 或是 (c, b)，或是 (c^{-1}, b)，而因为 c 与 b 可交换，这两者都是单位元素．于是 $(a^i, b) = 1 = (a, b)^i = c^i$．因此 $c^i = 1$ 而且 $a^{ri} = 1$，$b^{si} = 1$．因此 H 中不能交换的两个元素都是有限阶的．如果 H 的元素 x 同时与 a 和

1) 如果一个群 G 的非单位元素的阶都是 p，则 p 叫做群 G 的方次数．——译者

b 可交换，则 xa 不与 b 可交换，由此得出 xa（因而还有 x）是有限阶的．因此 H 的每个元素都是有限阶的．

设 a 和 b 是 H 的不可交换的元素，而且 $a^N=1, b^M=1$．这里假定 N 和 M 都是极小的．如果 p 是 N 的任意素约数，则根据 N 的极小性，a^p 与 b 可交换，因而 $(a^p,b)=(a,b)^p=1$．对于 M 的任意素约数有同样的结果．因为 $c=(a,b)\neq 1$，只能有一个素数同时整除 M 和 N，因而 $M=p^m, N=p^n$．因此 $a^{p^n}=1$，$b^{p^m}=1$，$c=(a,b)$，$c^p=1$，这里不妨假定 $n\geqslant m$．再有，因为 $c\in\{a\}$ 和 $c\in\{b\}$，所以

$$c=a^{jp^{n-1}}=b^{kp^{m-1}},$$

这里 $j, k\not\equiv 0 \pmod p$．

在 $\{a,b\}$ 内导出群是 $\{c\}$ 而且在它的中心内．因而在 $\{a,b\}$ 内，权等于或大于 3 的换位子是单位元素．我们可以用归纳法建立公式

$$(ab)^i=a^ib^i(b,a)^{i(i-1)/2}.$$

这在 $i=1$ 时成立，而且我们有

$$\begin{aligned}(ab)^{i+1}&=(ab)^iab=a^ib^i(b,a)^{i(i-1)/2}ab\\&=a^ib^iab(b,a)^{i(i-1)/2}=a^iab^i(b^i,a)b(b,a)^{i(i-1)/2}\\&=a^{i+1}b^i(b,a)^ib(b,a)^{i(i-1)/2}=a^{i+1}b^{i+1}(b,a)^{(i-1)/2}.\end{aligned}$$

用归纳法证明的这个公式对于任何这样的群 $\{a,b\}$ 都成立，只要 (a,b) 在它的中心内．这个公式也是集积公式的一个推论．

如果 $b_1=a^ub^k$，这里 $u=-jp^{n-m}$，则 $\{a,b_1\}=\{a,b\}$，因而 b_1 不与 a 可交换，因此根据假设，b_1 的阶不会低于 b 的阶．刚才建立的公式给出

$$\begin{aligned}b_1^p&=(a^ub^k)^p=a^{up}b^{kp}(b^k,a^u)^{p(p-1)/2}\\&=a^{pu}b^{kp}c^{-ukp(p-1)/2},\end{aligned}$$

因而

$$b_1^{p^{m-1}} = a^{-ip^{n-1}} b^{kp^{m-1}} c^{ikp^{n-1}(p-1)/2} = c^{ikp^{n-1}(p-1)/2}.$$

这里 $b_1^{p^{m-1}} \neq 1$,但是由于 $c^p = 1$,我们必定有 $p = 2$, $n = 2$. 因而 a 和 b 所满足的关系是 $a^2 = b^2 = a^{-1}b^{-1}ab = c$, $c^2 = 1$, 而且 $\{a, b\}$ 是四元数群. 这证明了H的任何非阿贝尔的子群都包含四元数群.

其次我们来证明,H是四元数群Q和Q在H内的中心化子的群 Z 的併,这里 Q 由 $a^4 = b^4 = 1$, $a^2 = b^2$, $ba = a^{-1}b$ 决定.如果H的元素 x 不与 a 可交换,则 $x^{-1}ax = a^{-1}$ 而且 xb 与 a 可交换.同理,如果 x (或 xb)不与 b 可交换,则 xa (或 xba) 与 a 可交换. 因此元素 x, xb, xa, xba 中的一个在Z内. 因此 $H = Q \cup Z = QZ$.现在我们来证明Z不能包含 4 阶元素.事实上,如果 $x^4 = 1$, $x \in Z$,则 $(a, bx) \neq 1$. 因为 $(bx)^4=1$, 我们有 $a^{-1}(bx)a = (bx)^{-1}$, 因而 $a^{-1}bax = b^{-1}x^{-1}$, 这给出 $x^2 = 1$. 因为 Z 不包含 4 阶元素, Z 不能包含四元数群, 所以 Z 是阿贝尔群, 并且 $Z \cap Q = \{a^2\}$. 利用左恩引理可以找出 Z 的子群 Z_1,它对于不包含 a^2 的性质而说是极大的. 然后我们容易得出 $Z = Z_1 + Z_1a^2$, $H = Q \times Z_1$. Z_1 是每个元素都是奇数阶的阿贝尔群U和方次数为 2 的阿贝尔群 V 的直积,因为 Z_1 不包含 4 阶元素. 因此 $H = Q \times U \times V$.

反之, 形状为 $Q \times U \times V$ 的群是哈密尔顿群. 因为Q不是阿贝尔群, 只要证明每个循环子群$\{quv\}$都是正规子群就够了. U和V都在 $Q \times U \times V$ 的中心内, 因而我们只要证明 a 和 b 都把上述子群变成自己.这时 $a^{-1}(quv)a = q^iuv$, 这里 $i = 1$ 或 3. u 的阶是奇数 n, 而 v 的阶是 2. 因此同余式 $r \equiv i \pmod 4$ 和 $r \equiv 1 \pmod n$ 都可解,而且

$$a^{-1}(quv)a = (quv)^r.$$

这就证明了我们的定理.

第十三章　阿贝尔群理论的继续

13.1. 加法群．群取模 1

任何群都可以用加法来表出群运算．大家习惯于用加法表出阿贝尔群，这在存在算子时特别方便．同时在熟知的体系的加法中自然地产生了一些群．我们在这里要考虑两个群：有理数加法群 r_+ 和实数加法群 R_+.

在用加法记号表出群时，我们将适当地改变术语，把积改成和而说成元素的和，笛卡儿和，以及直和．

用加法表出的循环群由生成元素 a 的全体整倍数 na 组成．群 r_+ 和 R_+ 都是无周期的，因为从 $na=0$ 得出 $a=0$. 在由 a 生成的无限循环群内，不存在使 $2x=a$ 的元素 x. 因为对于 r_+ 内的任何 a，存在使 $2x=a$ 的 x，所以 r_+ 不是循环群．但是 r_+ 非常接近于循环群．r_+ 中的任何有限元素组生成循环群．为了描述这个性质，我们说 r_+ 是秩为 1 的或局部循环的．更一般地，我们说一个阿贝尔群是秩为 k 的，假如由任何有限个元素生成的子群都能由不多于 k 个的元素生成，并且存在有限生成的子群，它必须有 k 个生成元素．

定理 13.1.1. 有理数加法群 r_+ 是局部循环群．

证明．考虑 r_+ 的由有限个元素 $a_1/b_1, \cdots, a_t/b_t$ 生成的子群．它的元素是这样的数 $m_1a_1/b_1+\cdots+m_ta_t/b_t$，这里 m_i 都是任意整数．这些数可以改写成 $(m_1a_1b_2\cdots b_t+\cdots+m_ta_tb_1\cdots b_{t-1})/b_1b_2\cdots b_t$. 这时我们容易验证分子组成整数加法群的加法子群，它是循环群．这个循环群由某个整数 w 的

全体整倍数组成. 因此已知群由数 $nw/b_1b_2\cdots b_t$ 组成，它是循环群.

在群 R_+ 中全体整数组成子群，它作为阿贝尔群的子群是正规子群. 在对应的商群中，相差一个整数的全体元素等同了起来，因而我们把商群说成群 R_+ 取模 1. 同理 r_+ 有一个商群是群 r_+ 取模 1，它当然是群 R_+ 取模 1 的子群.

群 $r_+(\mathrm{mod}\ 1)$ 是周期群，因为设 a/b 是任何有理数(a, b是整数)，我们有 $b(a/b)\equiv 0(\mathrm{mod}\ 1)$. 根据定理 3.2.3，$r_+(\mathrm{mod}1)$ 是它的西罗子群 $S(p)$ 的直和. 我们把 $r_+(\mathrm{mod}\ 1)$ 的西罗子群 $S(p)$ 记做 $Z(p^\infty)$. $Z(p^\infty)$ 由无限集合 $1/p, 1/p^2, \cdots, 1/p^i\cdots(\mathrm{mod}\ 1)$生成. $Z(p^\infty)$的元素有形状 $m/p^n, (m, p)=1$，而且这个元素生成的循环群与 $1/p^n$ 生成的相同. 因此 $Z(p^\infty)$ 的子群或是有限群，或者包含集合 $1/p, 1/p^2, \cdots, 1/p^i\cdots(\mathrm{mod}\ 1)$ 中的无限个元素，因而它是整个群 $Z(p^\infty)$. 因此 $Z(p^\infty)$ 是这样的无限群，它的所有真子群都是有限的循环群.

13.2. 阿贝尔群的特征标. 阿贝尔群的对偶

给了任意的阿贝尔群 A. A 的**特征标** χ 是从 A 到群 $R_+(\mathrm{mod}\ 1)$ 的同态. 因而根据定义有

$$\chi(a_1)+\chi(a_2)=\chi(a_1+a_2)\quad \text{对于所有 } a_1, a_2\in A. \tag{13.2.1}$$

这里加法 a_1+a_2 是在 A 内的加法，而特征标的值的加法当然是在 $R_+(\mathrm{mod}\ 1)$ 内. 我们还要定义特征标的加法. 如果 χ_1 和 χ_2 是 A 的两个特征标，我们定义

$$\chi_3(a)=\chi_1(a)+\chi_2(a)\quad \text{对于所有 } a\in A, \tag{13.2.2}$$

则 χ_3 也是 A 的特征标，因为

$$
\begin{aligned}
\chi_3(a_1+a_2) &= \chi_1(a_1+a_2)+\chi_2(a_1+a_2)\\
&= \chi_1(a_1)+\chi_1(a_2)+\chi_2(a_1)+\chi_2(a_2)\\
&= \chi_1(a_1)+\chi_2(a_1)+\chi_1(a_2)+\chi_2(a_2)\\
&= \chi_3(a_1)+\chi_3(a_2). \qquad (13.2.3)
\end{aligned}
$$

容易验证，如果利用（13.2.2）定义加法

$$\chi_3=\chi_1+\chi_2, \qquad (13.2.4)$$

则相对于加法（13.2.4），全体特征标组成加法群 A^*，它的零元素是把 A 的每个元素都映成零的特征标.

定理 13.2.1. 有限阿贝尔群 A 的特征标群 A^* 同构于 A.

证明. 对于任何同态都有 $\chi(0)=0$. 因此对于有限 m 阶元素 a，我们有 $m\chi(a)=\chi(ma)=0$. 因此 $\chi(a)$ 必定是 m 个值 $0, 1/m, \cdots, (m-1)/m \pmod 1$ 中的一个. 有限阿贝尔群的特征标显然由它对于基底的值完全决定. 设 a_i（$i=1, \cdots, r$）是 A 的基底，这里 a_i 的阶是 n_i，因而 A 的阶是 $n=n_1n_2\cdots n_r$. 因为 $\chi(a_i)$ 最多有 n_i 个可能，所以最多存在 A 的 $n=n_1n_2\cdots n_r$ 个特征标. 而我们容易证明恰好存在这么多个特征标. 因为如果我们令 $\chi_i(a_i)=1/n_i$，$\chi_i(a_j)=0$ 对于 $j\neq i$，则就可以证明，对于每个 $i=1, \cdots, r$，这决定一个特征标，而且对应 $a_i \rightleftarrows \chi_i$ 决定 A 和 A^* 之间的同构. 然而 A 和 A^* 之间的同构并不唯一决定，而取决于 A 的基底的特殊选取.

下列定理对于不论是否有限的阿贝尔群都成立：

定理 13.2.2. 设 H 是阿贝尔群 A 的子群. 那么对于每个 $h\in H$ 都有 $\chi(h)=0$ 的 A 的特征标 χ 所成的群同构于商群 A/H 的特征标群.

证明. 如果一个特征标对 H 的每个元素取值 0，则它对于傍系 $H+x$ 的每个元素取同一个值. 我们可以认为作为商群 A/H 的元素的傍系在 $R_+ \pmod 1$ 中对应于这个值. 容易

验证这是 A/H 的特征标. 反之,同态 $A \to A/H$ 和从 A/H 到 $R_+ \pmod 1$ 的同态的合成是从 A 到 $R_+ \pmod 1$ 的同态. 这样得到的 A 的特征标通过把 H 的元素映到 A/H 的零而后映到 $R_+ \pmod 1$ 的 0.

推论 13.2.1. 如果在有限阿贝尔群 A 内 $a \neq 0$,则存在使 $\chi(a) \neq 0$ 的 A 的特征标 χ.

因为如果不是这样,则 A 的每个特征标都是商群 $A/\{a\}$ 的特征标. 于是根据定理 12.3.1, A^* 将同时同构于 A 和 $A/\{a\}$,然而后者有较低的阶.

群 A 和 B 之间的对偶是在 A 的子群 H 和 B 的子群 K 之间的一一对应 $H \rightleftarrows K$,这时对应的群有相反的包含关系,这就是说,如果 $H_1 \rightleftarrows K_1$ 和 $H_2 \rightleftarrows K_2$ 而且 $H_1 \supset H_2$,则 $K_1 \subset K_2$,反之,如果 $K_1 \subset K_2$, 则 $H_1 \supset H_2$. 在有限阿贝尔群 A 和它的特征标群 A^* 之间存在自然的对偶,这就是下面的定理.

定理 13.2.3. 在有限阿贝尔群 A 和它的特征标群 A^* 之间存在着由子群的对应 $H \rightleftarrows K$ 决定的对偶, 这里给定 A 的子群 H, K 由对于每个 $h \in H$ 都有 $\chi(h) = 0$ 的 A 的特征标 χ 组成,又给定 A^* 的子群 K,H 由对于每个 $\chi \in K$ 都有 $\chi(h) = 0$ 的 A 的元素 h 组成. 又 A 与自己成对偶.

证明. 对于 A 的每个子群 H,我们取对于每个 $h \in H$ 都有 $\chi(h) = 0$ 的 χ 组成的 A^* 的子群 H^* 与它对应. 如果 $H_1 \neq H_2$ 是 A 的两个不同的子群,则 H_1 和 H_2 中的一个 (例如 H_1) 包含不属于另一个的元素 b. 于是根据定理 13.3.2, H_2^* 是 A/H_2 的特征标群,而且根据推论 13.2.1, 存在 $\chi \in H_2^*$ 使得 $\chi(b) \neq 0$. 因此 $H_1^* \neq H_2^*$. 因为 A 和 A^* 是有限的而且同构的, 所以 $H \to H^*$ 是在 A 的子群和 A^* 的子群之间的一一对应,特别说来, A^* 的每个子群 K 是对应于 A 的唯一子群 H 的子群 $K = H^*$. 如果 $H_1 \rightleftarrows K_1 = H_1^*$ 和 $H_2 \rightleftarrows K_2 = H_2^*$,则从 $H_1 \supset H_2$ 得

出 $K_1 \subset K_2$，因为当对于每个 $h \in H_1$ 都有 $\chi(h) = 0$ 时，当然得出对于每个 $h \in H_2 \subset H_1$ 都有 $\chi(h) = 0$. 同理从 $K_1 \subset K_2$ 得出 $H_1 \supset H_2$. 因而定理中的对应是在 A 和 A^* 之间的对偶. 于是在 A 和 A^* 之间的同构就导出 A 与自己的对偶.

定理 13.2.4. 如果阿贝尔群 A 是周期群而且它的全体西罗子群都是有限群，则它是自成对偶的.

证明. 如果 A 是周期阿贝尔群而且它的西罗子群都是有限群，则西罗子群 $S(p)$ 作为有限群是自成对偶的. 我们把它记做 $H_p \rightleftarrows H_p^d$，这里对于 $S(p)$ 的每个子群 H_p，对偶子群是 H_p^d. 现在如果 H 是 A 的任何子群，则 H 是它的西罗子群 H_p 的直和. 然后令 $H^d = \sum_p H_p^d$. 容易验证这是 A 的对偶. 注意这个论断并不适用于未加限制的任意有限阿贝尔群的直和，因为一般地说，这种直和可以具有这样的子群，它们不是加项的子群的直和. 白尔 (Baer[6]) 曾经证明过，自成对偶的阿贝尔群恰好就是定理里所说的那种阿贝尔群.

13.3. 可　除　群

用加法表示的阿贝尔群 A 叫做可除的，假如对于每个 $a \in A$ 和整数 n，存在元素 $x \in A$，使得 $nx = a$.

定理 13.3.1. 可除群是包含它的每个阿贝尔群 A 的直接加项.

证明. 设给了阿贝尔群 A 和可除子群 D. 需要证明存在子群 B，使得

$$A = D \oplus B, \text{或者 } D \cap B = 0 \text{ 而且 } D \cup B = A. \quad (13.3.1)$$

为了证明这一点，最好利用在 §1.8 里介绍过的左恩引理. 如果 $U_1 \subset U_2 \subset U_3 \subset \cdots$ 是 A 的子群的递升链，这里 $D \cap U_i = 0$，

则 $U = \bigcup_i U_i$ 也具有性质 $D \cap U = 0$. 因此根据左恩引理，A 包含子群 K，它对于性质 $K \cap D = 0$ 而说是极大的. 如果能证明 $D \cup K = A$，则就可以在 (13.3.1) 中取 $B = K$. 设 x 是 A 的不属于 $K \cup D$ 的元素. 那么根据 K 的极大性，$\{x\} \cup K$ 与 D 有公共的非零元素. 因此对于某个非负整数 n 和 $k \in K$，我们有 $nx + k = d \in D$, $d \neq 0$. 这时 $n \neq 0$，因为 $D \cap K = 0$. 又如果 $n = 1$，则 $x \in K \cup D$ 而与假设矛盾. 因为 D 是可除群，$d = nd_1$，这里 $d_1 \in D$，而且 $n(x - d_1) = -k$. 令 $x_1 = x - d_1$，那么当 $x_1 \in K \cup D$ 时，也有 $x \in K \cup D$ 而与假设矛盾. $K \cup \{x_1\}$ 的元素有形状 $mx_1 + k$, $0 \leqslant m < n$. 根据 K 的极大性，必定存在 $\{x_1\} \cup K$ 和 D 的公共元素 $n_1x_1 + k_1 = d = n_1d_2$，这里 $n_1 < n$, d, $d_2 \in D$. 这时取 $x_2 = x_1 - d_2$，我们有 $n_1x_2 = -k_1 \in K$，而且当 $x_2 \in K \cup D$ 时还有 $x_1 \in K \cup D$ 而与假设矛盾. 继续这个步骤. 最终地得出一个 $n_i = 1$，于是 x_i, x_{i-1}, $\cdots$, x_1 和 x 都属于 $K \cup D$ 而与假设矛盾. 因此 $K \cup D = A$，定理证明了.

在卡泼伦斯基的专著 (Kaplansky[1]) 里证明了：每个可除群是同构于 r_+ 或群 $Z(p^\infty)$ 的群的直和.

13.4. 纯 子 群

我们把 H 叫做阿贝尔群 A 的**纯子群**，假如对于任意整数 n 和 $h \in H$，从满足 $nx = h$ 的 $x \in A$ 的存在得出满足 $nh_1 = h$ 的 $h_1 \in H$ 的存在. 因此纯性是一种相对的可除性：要 H 内的可除性成立，只要它在整个群内成立. 可除群当然是包含它的任何阿贝尔群的纯子群. 直接加项是纯子群. 但是可除群必定是无限群，而有限群却可以是纯子群，因此这概念在研究有

限群时是有用的.

阿贝尔群的周期子群[1]是纯子群,因为如果 $nx = h$ 中的 h 是有限阶的,则当 x 存在时,它必定也是有限阶的. 纯子群的递升链的并集是纯子群,因为如果 h 是这併集的元素,则 h 是链中某个群的元素,因而 $nx = h$ 在链中有解.

定理 13.4.1 指出,在很多情形下,纯子群是直接加项.

定理 13.4.1. 设 A 是阿贝尔群, H 是纯子群, 又设 A/H 是循环群的直和. 那么 H 是 A 的直接加项.

证明. 我们先证明一个引理.

引理 13.4.1. 如果 H 是 A 的纯子群而且 y 是 A/H 的元素,则就存在 A 的与 y 有相同的阶的元素 x, 它在同态 $A \to A/H$ 下被映成 y.

如果 y 是无限阶的, 则映成 y 的任何 x 都与 y 同阶. 如果 $ny = 0$ 而且 $u \to y$, 则 $nu \to 0$, $nu = h \in H$. 于是根据 H 的纯性, $h = nh_1$. 这时令 $x = u - h_1$. 那么 $x \to y$ 而且 $nx = n(u - h_1) = nu - nh_1 = h - h = 0$,这就是所要证明的.

定理的证明现在就很简单了. 设 A/H 是由基元素 $y_i (i \in I)$ 生成的循环群的直和. 在 A 中取元素 $x_i \to y_i$,而且我们总取 x_i 与 y_i 同阶,这种取法由引理保证它的可能. 设 K 是由 x_i 生成的子群. 如果在 A 内有关系 $n_{i_1}x_{i_1} + \cdots + n_{i_s}x_{i_s} = h \in H$, 则在 A/H 内就有 $n_{i_1}y_{i_1} + \cdots + n_{i_s}y_{i_s} = 0$,于是因为 y_i 是 A/H 的基元素,我们有 $n_{i_1}y_{i_1} = \cdots = n_{i_s}y_{i_s} = 0$. 而因为 x_i 与 y_i 同阶,所以 $n_{i_1}x_{i_1} = \cdots = n_{i_s}x_{i_s} = 0$,因而 $h = 0$. 因此 $K \cap H = 0$. 又 $K \cup H = A$, 因为 K 包含 A 对 H 的每个傍系的一个元素. 总之 $A = H \oplus K$,这就是要求证明的.

---

1) 指极大周期子群,即全体有限阶元素的集合.——俄译本编者注

13.5. 一 般 注 解

希望更详细地探讨阿贝尔群的读者可以去看卡泼伦斯基的专著(Kaplancky[1])和库罗什的书 (Kurosch [Курош][2]). 卡泼伦斯基的专著中特别有用的是阐述文献的一节.

一般地说,定理 3.2.3 把周期群的研究简化成本原群的研究. 关于本原群的主要结果之一是乌勒姆定理, 它以称为群的“乌勒姆不变量”的某种基数完全判定了可数本原阿贝尔群.

无限循环群的直和叫做自由阿贝尔群. 具有 r 个生成元素的阿贝尔群是具有 r 个生成元素的自由阿贝尔群的同态像. 循环群的直接和的每个子群本身是循环群的直和, 特别地说,自由阿贝尔群的子群是自由阿贝尔群.

在 § 13.3 中提出过,可除群是同构于 r_+ 的群和同构于各个 $Z(p^\infty)$ 的群的直接和. 阿贝尔群可以嵌入可除群,所以在某种意义下, 研究阿贝尔群可以看作是研究可除群的子群. 因而秩为 1 的不挠 (即无周期) 群是 r_+ 的子群.

同时包含有限阶和无限阶元素的阿贝尔群叫做混合群. 有例子可以说明混合群一般不是它的周期子群和不挠群的直和. 但是因为周期子群是纯子群, 所以定理 13.4.1 已经指出混合群可以分解成周期部分和另一个群的直和.

第十四章　单项表示和转移

14.1. 单项置换

考虑未知数 $u_1, \cdots, u_n$ 的集合 S, 在这些未知数之左可以乘上群H的元素,满足下列定律:

$$1u_i = u_i, \tag{14.1.1}$$

这里 1 是H的单位元素;又

$$h_1(h_2u_i) = (h_1h_2)u_i.$$

单项置换M是指映射 $u_i \to h_{ij}u_j$, $i = 1, \cdots, n$, $j = j(i)$, 这里 $u_i \to u_j$ 是S的置换. 对于两个映射 $M_1: u_i \to h_{ij}u_j$ 和 M_2: $u_j \to h_{jk}u_k$, 我们定义它们的乘积是 $M_1M_2: u_i \to (h_{ij}h_{jk})u_k$. 在这个定义下，这些映射组成一个群，它的单位元素是映射 $u_i \to u_i$. 如果我们令映射 $M_1: u_i \to h_{ij}u_j$ 对应于矩阵 (h_{ij}), 它的第 i 行的第 j 个元素是 h_{ij}, 其他元素都是零，则映射相乘的法则正是普通的矩阵乘法.

在全体单项置换的群M中,乘法 $u_i \to h_{ii}u_i$ 组成正规子群 D, 而且商群 M/D 是 $u_1, \cdots, u_n$ 的置换的对称群. 更一般地,如果G是M的子群, 则当 $g \in G$ 是映射 $u_i \to h_{ij}u_j$ 时, $g \to g^*: u_i \to u_j$ 是从G到一个置换群上的同态，这个同态的核是 $G \cap D$.

我们说单项置换群G是传递的，假如对应的置换群是传递的.

定理 14.1.1. 设 K 是G的子群而且 $G = K + Kx_2 + \cdots + Kx_n$, 又设 $K \to H$ 是从K到群H上的同态. 那么G在H

上的传递的单项表示由下列方式给出：对于 $g\in G$，设 $x_ig=h_{ij}x_j$，$i=1,\cdots,n$，$j=j(i)$，$k_{ij}\in K$. 再设在同态 $K\to H$ 下有 $k_{ij}\to h_{ij}$. 那么 $\pi(g):u_i\to h_{ij}u_j$ 是 G 在 H 上的传递的单项表示. 反之，每个传递的单项表示或是这种类型的，或者在群 D 下共轭于这种类型的表示.

证明. 给了 G，G 的左傍系表达式 $G=K+Kx_2+\cdots+Kx_n$ 和同态 $K\to H$. 设 g_1 和 g_2 是 G 的任意两个元素. 那么当 $x_ig_1=k_{ij}x_j$ 和 $x_jg_2=k_{js}x_s$ 时，我们有 $x_i(g_1g_2)=k_{ij}k_{js}x_s$，因而对于对应的单项表示有 $\pi(g_1g_2)=\pi(g_1)\pi(g_2)$，即它确实是群 G 的表示(当然不一定是一一的). 对应的置换群是在 §5.3 中讨论过的左傍系的置换群，它当然是传递的.

反之，我们考虑 G 的任何传递的单项表示 R，对于 $g\in G$，$g\to\pi(g):u_i\to h_{ij}u_j$. 取定字母 u_1 来考虑 G 的全体这样的元素 k，$\pi(k)$ 把 u_1 映成 $h_{11}u_1$，这里 $h_{11}\in H$. 这些元素组成子群 K. 根据 R 的传递性，对于每个 $i=2,\cdots,n$，存在元素 x_i，使得 $\pi(x_i)$ 把 u_1 变成 $h_{1i}u_i$. 然后容易得出

$$G=K+Kx_1+\cdots+Kx_n. \qquad (14.1.2)$$

如果我们用元素 $d:u_1\to u_1,\cdots,u_i\to h_{1i}^{-1}u_i$ 来作 R 的变形，则在 $d^{-1}Rd$ 内有 $d^{-1}\pi(x_i)d$ 把 u_1 变成 u_i. 我们来讨论 $R^*=d^{-1}Rd$. 这时如果对于 $k\in K$，$\pi(k)$ 把 u_1 变成 hu_1，则 $\pi(x_i^{-1}kx_i)$ 把 u_i 变成 hu_i，反之亦然. 因而在表示 R^* 下作为系数而出现的每个 h 是 K 的元素的像. 这些 h 可能组成原先的群 H 的子群 H_1. 但是如果 $\pi(k)$ 把 u_1 变成 hu_1，则 $k\to h$ 是从 K 到 H_1 上的同态. 其次，如果 $\pi(g)$ 把 u_i 变成 $h_{ij}u_j$，则 $\pi(x_igx_j^{-1})$ 把 u_1 变成 $h_{ij}u_1$，因而 $x_igx_j^{-1}=k_{ij}\in K$ 而且映射 $k_{ij}\to h_{ij}$ 是从 K 到 H_1 上的同态.

注意在更换 G 对于 K 的左傍系代表时，就产生另一个单项表示，它在群 D 下共轭于前一个表示.

14.2. 转　移

设给了群G在群H上的单项表示R:

$$\pi(g): u_i \to h_{ij}u_j, \quad i=1,\cdots,n, \quad j=j(i). \qquad (14.2.1)$$

再设未知数的个数n是有限的. 那么容易验证映射

$$g \to \prod_{i=1}^{n} h_{ij} (\bmod H') \qquad (14.2.2)$$

是从G到商群H/H'上的同态，这里H'是H的导出群. 我们特别取$H=K$的情形:

$$G = K + Kx_2 + \cdots + Kx_n. \qquad (14.2.3)$$

这时如果$\phi(z)=x_j$对于$z=kx_j$, $k\in K$, 则我们有

$$V_{G\to K}(g) \equiv \prod_{i=1}^{n} x_i g \phi(x_i g)^{-1} (\bmod K'), \qquad (14.2.4)$$

而且$V_{G\to K}(g)$是从G到K/K'的同态. 这个同态叫做从群G到K的**转移**. 如果H是K的同态像，则映射(14.2.2)是到转移的像的同态映射，因为当$K\to H$时，K/K'映成H/H', K'是K的完全不变子群. 转移的主要性质由定理14.2.1给出.

定理 14.2.1.

1) **映射**$g\to V_{G\to K}(g)$**是从**G**到**K/K'**的同态**.

2) **转移**$V_{G\to K}(g)$**不依赖于代表元素**x_i**的选取**.

3) **如果**$G\supset K\supset T$, **则**$V_{G\to K}(g) = V_{K\to T}[V_{G\to K}(g)]$.

证明. 我们已经知道第一个性质是单项表示理论的一个推论. 但是我们将从转移的定义(14.2.4)直接证明全部三个性质. 对于第一个性质，我们注意到，如果$x_i g_1 = k_{ij}x_j$, $i=1,\cdots,n$, $x_j g_2 = k_{js}x_s$, $j=1,\cdots,n$, 则

$$V_{G\to K}(g_1) \equiv \prod_i k_{ij} (\bmod K'), \quad V_{G\to K}(g_2) \equiv \prod_j k_{js} (\bmod K'),$$

而且

$$V_{G\to K}(g_1g_2) \equiv \prod_i (k_{is}^*)(\mathrm{mod}\ K'),$$

这里 $k_{is}^* = k_{ij}k_{js}$. 对于第二个性质,如果 $x_i^* = a_ix_i$ 是代表的第一种和第二种选择之间的关系而且 $x_ig = k_{ij}x_j$, 则 $x_i^*g = a_ix_ig = a_ik_{ij}x_j = a_ik_{ij}a_j^{-1}x_j^*$; 于是在第一种情形下,

$$V(g) \equiv \prod_i k_{ij}(\mathrm{mod} K'),$$

在第二种情形下

$$V(g) \equiv \prod_i (a_ik_{ij}a_j^{-1}) \equiv \prod_i a_i \cdot \prod_i k_{ij} \prod_j a_j^{-1} \equiv$$

$\prod_i k_{ij}(\mathrm{mod} K')$. 对于第三个性质,设

$$G = K + Kx_2 + \cdots + Kx_n, \qquad (14.2.5)$$
$$K = T + Ty_2 + \cdots + Ty_m.$$

那么

$$\begin{aligned} G = T &+ Ty_2 + \cdots + Ty_m \\ &+ \cdots \\ &+ Tx_i + Ty_2x_i + \cdots + Ty_mx_i \\ &+ \cdots \\ &+ Tx_n + Ty_2x_n + \cdots + Ty_mx_n. \end{aligned}$$

这时对于 $g\in G$, 设 $x_ig = k_{ij}x_j$ 和 $y_rk_{ij} = t_{ijrs}y_s$. 那么 $y_rx_ig = t_{ijrs}y_sx_j$. 于是

$$V_{G\to T}(g) \equiv \prod_{i,r} t_{ijrs}(\mathrm{mod}\ T')$$

而且

$$V_{G\to K}(g) \equiv \prod_i k_{ij}(\mathrm{mod} K').$$

其次

$$V_{K\to T}(k_{ij}) \equiv \prod_r t_{ijrs}(\mathrm{mod}\ T'),$$

因此

$$V_{K\to T}(g) \equiv \prod_i V_{K\to T}(k_{ij})(\mathrm{mod} T')$$

$$\equiv V_{K\to T}(\prod_i k_{ij})(\mathrm{mod} T') \equiv V_{K\to T}[V_{G\to K}(g)].$$

我们注意到，因为从K到T上的转移把K'映成单位元素群，所以也可以说从$V_{G\to K}(g)$到T的转移，虽然这时提到的是K/K'的元素而不是K的元素.

14.3. 伯恩赛德定理

定理 14.3.1. 如果有限群G的西罗子群P在它的正规化子的中心内，则G有一个正规子群H，它以P的元素作为它的傍系代表.

证明. 我们从一个引理开始.

引理 14.3.1. 如果两个集合K_1和K_2在G的西罗子群P内不变而且在G内共轭，则K_1和K_2在$N_G(P)$内共轭.

引理的证明. 设$x^{-1}K_1x = K_2$，这里$x\in G$. 因为K_1在P内不变，所以$K_2 = x^{-1}K_1x$在$x^{-1}Px = Q$内不变. 因而P和Q都包含在K_2的正规化子内，因此它们作为西罗子群在$N_G(K_2)$内是共轭的. 于是$y^{-1}Qy = P$，这里y是使$y^{-1}K_2y = K_2$的元素. 因而对于$z = xy$，$z^{-1}Pz = P$，$z^{-1}K_1z = K_2$，这就证明了引理.

现在来证明定理. 因为P包含在$N_G(P)$的中心内，所以P是阿贝尔群而且$P' = 1$. 我们考虑$V_{G\to P}$. 设$u\in P$. 为了计算$V_{G\to P}(u)$，取P在G内的傍系代表为x_i, x_iu, $\cdots$, x_iu^{r-1}，这里$x_iu^r\in P_{x_i}$，而且当$j<r$时，$x_iu^j\notin Px_i$，这里对于$j<r$，$x_iu^{j-1}\cdot u\cdot(x_iu^j)^{-1} = x_iu^ju^{-j}x_i^{-1} = 1$，而且$x_iu^{r-1}\cdot u\cdot x_i^{-1} =$

$x_i u^r x_i^{-1}$. 因此，对于用 P 的左傍系的置换来表示 u 时的每个长度为 r 的圈，在关于 $V_{G\to P}(u)$ 的乘积中有一项是 $x_i u^r x_i^{-1}$，而其余都是单位元素. 因而

$$V_{G\to P}(u)=\prod_i x_i u^r x_i^{-1}.$$

其次，$x_i u^r x_i^{-1}\in P$ 在 G 内共轭于 u^r，因为 P 是阿贝尔群，这两个元素在 P 内都不变. 根据引理，$x_i u^r x_i^{-1}=y^{-1}u^r y$，这里 $y\in N_G(P)$. 根据假设，P 在它的正规化子的中心内，因而 $y^{-1}u^r y=u^r$. 因此 $V_{G\to P}(u)=\Pi u^r=u^n$，这里 $n=[G:P]$ 是所有的圈的长度的和. 因为 P 是阶为 p^s 的西罗子群，所以 $p\nmid n=[G:P]$. 因此，在从 G 到 P 上的转移下，P 同构地映成它自己而且 $V_{G\to P}(G)=P$，因为 $V_{G\to P}(G)$ 显然包含在 P 内. 这个同态的核必定是在 G 内有指数 p^s 而且阶为 $n=[G:P]$ 的群 H. 因此 H 是指数为 p^s 的正规子群，所以 P 的元素可以取作 H 的傍系代表.

推论 14.3.1. 有限单纯群的阶或者被 12 整除，或者被整除它的阶的最小素数的立方整除.

证明. 设 p 是整除单纯群 G 的阶的最小素数，再设西罗 p 子群 P 的阶是 p 或 p^2，因而它是阿贝尔群. 根据定理，如果 $N_G(P)$ 不导出 P 的非显然的自同构，则 G 具有同构于 P 的商群. 如果 P 的阶是 p，则它的自同构群的阶是 $p-1$，即小于 p. 如果 P 是 p^2 阶的循环群，则自同构群的阶是 $p(p-1)$，又如果 P 是 p^2 阶的非循环群，则这个阶等于 $(p^2-1)\cdot(p^2-p)=p(p-1)^2(p+1)$. 当 p 是奇数时，因为 $p+1=2[(p+1)/2]$，所以在这些因子中没有一个能被大于 p 的素数整除，因此 $N_G(P)$ 不能导出 P 的非显然的自同构. 如果 $p=2$，则在最后一个情形里 $p+1=3$，因而只有在 $N_G(P)$ 的阶能被12整除时，$N_G(P)$ 才能导出 P 的 3 阶的自同构.

14.4. P.赫尔、格润和维兰德的定理

下面几个定理的主要内容是在群G的西罗p子群和G的本身是p群的商群G/K之间的关系.

为了叙述这些关系,我们导入强闭和弱闭的概念.

定义. 设H是G的子群, B是H的子群. 如果对于任意$x\in G$, $H\cap B^x\subseteq B$, 这里$B^x=x^{-1}Bx$, 则B叫做在H内强闭的(相对于G而说);又如果从$B^x\subseteq H$得出$B^x=B$, 则B叫做在H内弱闭的.

我们说群G是p正规的, 如果西罗p子群P的中心Z是包含它的每一个西罗p子群P_1的中心. 这是弱闭性的特殊情形, 它相当于断定P的中心是在P内相对于G而弱闭的. 事实上,设G是p正规的. 再设$x\in G$使$Z^x\subseteq P$. 那么Z包含在$P_1=P^{x^{-1}}$内. 根据p正规性,Z是P_1的中心. 于是Z^x是$P_1^x=P$的中心,因而$Z^x=Z$, 所以Z在P内是弱闭的.反之,设Z在P内是弱闭的. 而且$Z\subseteq P_1$, P_1是另一个西罗子群. 那么对于某个$x\in G$, $P_1^x=P$. 于是$Z^x\subseteq P$. 根据弱闭性, $Z=Z^x$. 但是如果Z_1是P_1的中心,则Z_1^x是$P_1^x=P$的中心. 因此$Z_1^x=Z=Z^x$, 而且$Z=Z_1$是P_1的中心, 因而G是p正规的.

显然从强闭性得出弱闭性. H的弱闭的子群B在H内必定是正规的. 由满足某个方程$x^k=1$的全体x生成的H的子群是弱闭的,而如果这些x组成子群X, 则X在H内是强闭的. 当H是正规p群,以及在某些其他的条件下,出现的就是这种情形.

在不会引起混乱时,我们把转移$V_{G\to H}(g)$记做$V(g)$. 于是如果

$$G = H + Hx_2 + \cdots + Hx_n,$$

则

$$V(g) \equiv \prod_{i=1}^{n} x_i g \phi(x_i g)^{-1} (\mathrm{mod}\, H').$$

我们还可以把模 H' 的同余式换成模 H_0 的同余式，这里 H_0 是 H 的包含 H' 的子群，而且 H/H_0 是阿贝尔群. 以后用到的同余式都是取模 H_0 的.

对于 $g \in G$ 和 $i = 1, \cdots, n$，定义 ig 为使 $x_i g x_{ig}^{-1} \in H$ 的 $1, \cdots, n$ 中的一个. 那么对于固定的 g，$i \to ig$ 是 G 在 H 的左傍系上的传递的置换表示中的置换 $\pi(g)$. 因而我们记

$$V(g) \equiv \prod_i x_i g x_{ig}^{-1}.$$

置换 $\pi(g)$ 可以分解成一系列的圈，包括不变的文字作为长度为 1 的圈. 从每个圈取一个文字而且把它们组成的集合记做 $C_H(g)$. 对于 $i \in C_H(g)$，设 r_i 是 i 所在的圈的阶. 于是

$$\sum_{i \in C_H(g)} r_i = n,$$

这只不过是说圈的总长度是 n.

引理 14.4.1.

$$V(g) \equiv \prod_{i \in C_H(g)} x_i g^{r_i} x_i^{-1}.$$

这里 $x_i g^{r_i} x_i^{-1}$ 是在 H 内的 $x_i g x_i^{-1}$ 的最低方幂.

证明. 在 $\pi(g)$ 的以 i 开始的圈中有 $i, ig, \cdots, ig^{r_i-1}$ 全都不同，而且我们可以取 $x_i, x_i g, \cdots, x_i g^{r_i-1}$ 作为 H 的对应傍系的代表. 于是 $V(g)$ 中对应于具有文字 i 的圈的因子的乘积是

$$x_i g (x_i g)^{-1} \cdot (x_i g) g (x_i g^2)^{-1} \cdot (\cdots) \cdot (x_i g^{r_i-1}) g x_i^{-1}$$
$$= x_i g^{r_i} x_i^{-1},$$

因为 $\phi(x_i g^s) = x_i g^s$，$s = 1, \cdots, r_i - 1$，$\phi(x_i g^{r_i}) = x_i$. 又因为当 $s < r_i$ 时有 $x_i g^s \notin Hx_i$，所以 $x_i g^{r_i} x_i^{-1}$ 是属于 H 的

$x_i g x_i^{-1}$ 的最低方幂.

我们把 $V(g)$ 中对应于长度为 1 的圈的乘积叫做对角乘积 $d(g)$，而且记

$$d(g) \equiv \prod_{i=ig} x_i g x_i^{-1} (\mathrm{mod}\, H_0),$$

这时像 $V(g)$ 一样，$d(g)$ 取模 H_0 是与因子的阶和傍系代表 x_i 的选取无关的.

引理 14.4.2. 如果 u 和 v 在 G 内是共轭的，则 $d(u) = d(v)$. 又 $d(u^{-1}) = [d(u)]^{-1}$.

证明. 设 $v = t^{-1}ut$. 那么 $iu = i$ 等价于 $itv = it$，因而根据定义，

$$\begin{aligned} d(v) &\equiv \prod_{i=iu} x_{it} v x_{it}^{-1} \\ &\equiv \prod_{i=iu} (x_{it} t^{-1} x_i^{-1})(x_i u x_i^{-1})(x_i t x_{it}^{-1}) \\ &\equiv \prod_{i=iu} (x_i u x_i^{-1}) \equiv d(u). \end{aligned}$$

得出这个结果是因为 $x_{it}t^{-1}x_i^{-1}$ 和 $x_i t x_{it}^{-1}$ 属于 H 而且是彼此互逆的. 再有,因为 $i = iu$ 等价于 $i = iu^{-1}$, 所以

$$d(u^{-1}) \equiv \prod_{i=iu} s_i u^{-1} s_i^{-1} \equiv \left(\prod_{i=iu} s_i u s_i^{-1} \right)^{-1} \equiv [d(u)]^{-1}.$$

对于 $h \in H$ 定义 $d^*(h) \equiv h^{-1}d(h)$.那么根据引理 14.4.2, $h \equiv d(h)[d^*(h)]^{-1} \equiv d(h)d^*(h^{-1})$,而且$d(h^r) \equiv d(x_i h^r x_i^{-1})$. 因而如果 $x_i h^r x_i^{-1} \in H$, 则

$$x_i h^r x_i^{-1} \equiv d(h^r) d^*(x_i h^{-r} x_i^{-1}) \equiv h^r d^*(h^r) d^*(x_i h^{-r} x_i^{-1}).$$

所以根据引理 14.4.1, 我们有

引理 14.4.3. 如果 $h \in H$, 则

$$V(h) \equiv h^n \prod_{i \in C_H(h)} d^*(h^{r_i}) d^*(x_i h^{-r_i} x_i^{-1}).$$

推论 14.4.1. 如果 $d^*(h)\in H_0$ 对于所有 $h\in H$，则对于任何 $h\in H$，$V(h)=h^n$.

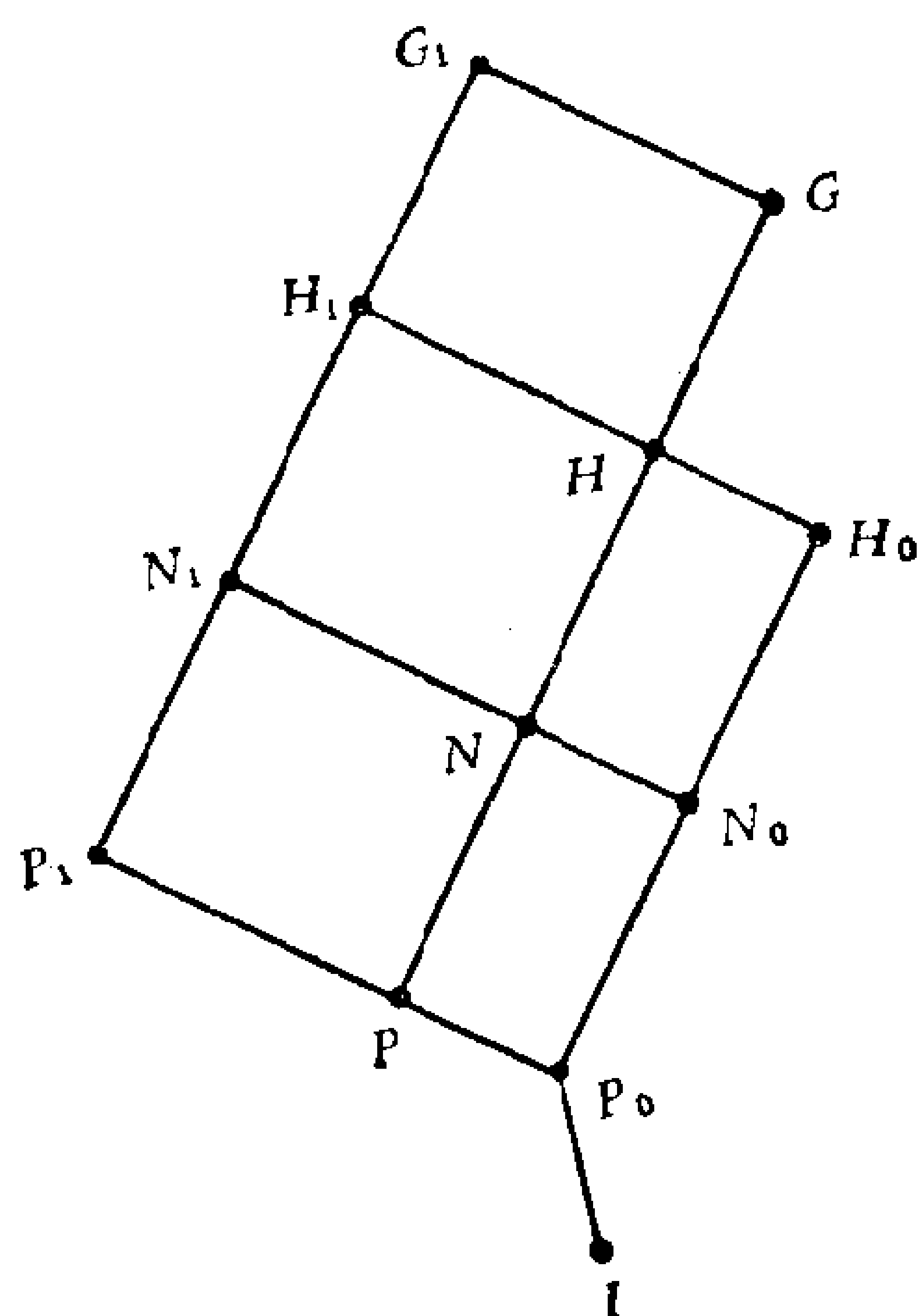


图 6 P. 赫尔定理

设 p 是素数，G_1 是有限群，又 $G=u_p(G_1)$ 是由 G_1 的全体这种元素生成的群，这种元素的阶与 p 互素. 因而 G_1/G 是 G_1 的极大的 p 商群. 设 P_1 是 G_1 的西罗 p 子群，N_1 是它在 G_1 内的正规化子，H_1 是 G_1 的包含 N_1 的任意子群. 令 $P=P_1\cap G$，$N=N_1\cap G$，$H=H_1\cap G$，于是 $G_1=GP_1=GN_1=GH_1$ 而且 $P_1/P=N_1/N=H_1/H=G_1/G$. G 是 G_1 的完全不变子群，P 是 G 的西罗 p 子群，N 包含在 P_1 和 G 的正规化子内，因而包含在 $P_1\cap G=P$ 的正规化子内. 于是因为 G 由阶与 p 互素的元素生成，所以 $u_p(G)=G$，但是可能有 $u_p(H)\subset H$. 假定 $u_p(H)\subset H$ 成立，于是 $u_p(H)$ 是 H 的完全不变子群，而 H 在 H_1 内是正规的. 因为 H_1/H 是 p 群，所以 $u_p(H)=u_p(H_1)$. 令

$$H_0=H^p\cup(H,H_1)\cup u_p(H)=H^p(H,H_1)u_p(H).$$

这里 H^p 是由 H 的元素的 p 次方幂生成的群，而 (H,H_1) 是由换位子 (h,h_1) 生成的群，这里 $h\in H$，$h_1\in H_1$. 因为 $H_1/u_p(H)$ 是 p 群，因而它是幂零的. 因此 $(H,H_1)/u_p(H)$ 是 $H/u_p(H)$ 的真子群. 其次，因为 H^p 包含在任何这样的子群 T 内，$H\supset T\supset(H,H_1)u_p(H)$ 而且 $[H:T]=p$，所以如果 $u_p(H)$ 是 H 的真子群，则 H_0 也是 H 的真子群，而且 H/H_0 是 p 群. 考

虑这样的问题：H_0 和 P 的什么样的元素共同生成 H?

引理 14.4.4. H 由 H_0 和 $u\in P$ 的全体元素 $d^*(u)$ 的集合共同生成.

证明. 像前面一样,我们有

$$G = H + Hx_2 + \cdots + Hx_n,$$
$$d(u) \equiv \prod_{i=iu} x_iux_i^{-1} \bmod H_0$$
$$d^*(u) \equiv u^{-1}d(u) \bmod H_0,$$

而且由于 $H_0 \supseteq (H, H_1) \supseteq (H, H) = H'$, 所以 H/H_0 是阿贝尔群. 因为 $u\in P\subseteq H$, 我们当然有全体 $d^*(u)\in H$. 因而 $K = \{d^*(u)|u\in P\}\cup H_0 \subseteq H$. 为了证明 $H\subseteq K$, 我们利用下列事实：因为 H/H_0 是阿贝尔 p 群，对于 G 的其阶与 p 互素的元素 w 有 $V(w)\equiv 1 \pmod{H_0}$. 但是根据构造，G 由这种元素生成. 因而对于每个 $u\in G$, 都有 $V(u)\equiv 1 \pmod{H_0}$. 因此对于每个 $u\in P$, 更有 $V(u)\in K$. 于是根据引理 14.4.3, 对于 $u\in P$ 有

$$V(u) \equiv u^n \prod_{i\in C_H(u)} d^*(u^{r_i})d^*(x_iu^{-r_i}x_i^{-1}).$$

这里根据定义，$d^*(u^{r_i})\in K$, 而且 $v = x_iu^{-r_i}x_i^{-1}$ 是 H 的阶为 p 的方幂的元素，因而对于某个 $y\in H$, $y^{-1}vy\in P$, 所以根据引理 14.4.2, $d^*(v) = v^{-1}d(v) = v^{-1}d(y^{-1}vy)$. 于是

$$d^*(v) \equiv v^{-1}y^{-1}vyd^*(y^{-1}vy) \equiv (v, y)d^*(y^{-1}vy).$$

但是根据定义，$(v, y)\in H'\subseteq H_0$ 而且 $d^*(y^{-1}vy)\in K$. 因而 $d^*(v) = d^*(x_iu^{-r_i}x_i^{-1})\in K$. 由此得出对于 $u\in P$ 有

$$u^n \equiv V(u)\in K.$$

但是 $(n, p) = 1$ 而且 P 的每个元素是 P 的某个别的元素的 n 次方幂. 因而 $P\subseteq K$. 又因为 H/H_0 是 p 群而且 P 是 H 的西罗 p 子群,所以 $H = H_0\cup P\subseteq K$. 因而 $H = K$. 这就证明了引理.

因为 $G \triangleleft G_1$ 而且 $H = H_1 \cap G$, $G \cup H_1 = G_1$, 我们可以利用H在G内的左傍系代表 $1, x_2, \cdots, x_n$ 作为 H_1 在 G_1 内的左傍系代表. 因而 $G_1 = H_1 + H_1x_2 + \cdots + H_1x_n$. 因此, G_1 用 H_1 和 P_1 的二重傍系表出是

$$G_1 = H_1 + H_1t_1P_1 + \cdots + H_1t_sP_1,$$

这里 $1, t_1, \cdots, t_s$ 是 $1, x_1, \cdots, x_n$ 的子集. 设 $\pi_i (i = 1, \cdots, s)$ 是 P_1 到 H_1 在 $H_1t_iP_1$ 内的傍系上的置换的传递表示. 这时 π_i 的次数大于 1, 因为否则 $H_1t_iP_1 = H_1t_i$, 于是 $t_iP_1t_i^{-1} \subseteq H_1$, 以致根据西罗定理,存在某个 $y \in H_1$ 使得 $t_iP_1t_i^{-1} = y^{-1}P_1y$, 由此得出 $yt_i \in N_1 \subseteq H_1$, 因而 $t_i \in H_1$, 这是不可能的. 因此 P_1 的表示 π_i 不是单位元素群,因而它的核 K_i 是 P_1 的真子群,而 π_i 一一地表示 P_1/K_i. 由于 P_1/K_i 是 p 群, 它的中心不是单位元素群. 因此我们可以取元素 $z_i \in P_1$, 使得 $\pi_i(z_i)$ 是 p 阶的而且在 $\pi_i(P_1)$ 的中心内. 这时对于每个 $u \in P_1$, $\pi_i(z_i)$ 与 $\pi_i(u)$ 都可交换. 在传递的置换群的中心内的元素, 如果不变一个文字,则就不变全体文字. 因此 $\pi_i(x_i)$ 改变 H_1 在 $H_1t_iP_1$ 中的每个傍系而完全由长度为 p 的圈组成. 对于任何 $u \in P \subseteq P_1$, $\pi_i(u)$ 与 $\pi_i(z_i)$ 可交换, 因而如果 $\pi_i(u)$ 不变包含在 $H_1t_iP_1$ 中的任何傍系, 例如 H_1x_{j+1}, 则它必定也不变 H_1x_{j+1} 所属的 $\pi_i(z_i)$ 的圈中的全体傍系 $H_1x_{j+1}, \cdots, H_1x_{j+p}$. 因此对于$u \in P$, 可以记

$$d(u) = u \cdot \Pi d_i(u) \bmod H_0,$$

这里

$$d(u) = h_1h_2 \cdots h_p,$$

而且

$$k_k = x_{j+k}ux_{j+k}^{-1}, \quad k = 1, \cdots, p,$$

这里 $x_{j+1}, \cdots, x_{j+p}$ 是对于某个 i 的 $\pi_i(z_i)$ 的一个圈中的傍系. 这时 $u = 1 \cdot u \cdot 1^{-1}$ 是 $d(u)$ 的属于 H_1 的唯一的因子.

我们还注意到，对于 $x_{j+k}ux_{j+k}^{-1}=h_k\in H_1$，因为 $x_{j+k}\in G$，$u\in P$，我们有 $h_k\in G$，因而 $h_k\in H_1\cap G=H$，所以这些确实是 $d(u)$ 中的因子. 现在从 $d^*(u)=u^{-1}d(u)$ 得出

$$d^*(u)\equiv\prod_j d_j(u)\ \mathrm{mod}\ H_0.$$

从这个关系和引理 14.4.4 立即得出：

引理 14.4.5. *H由H_0和$u\in P$的全体$d_j(u)$生成.*

详细地来讨论这些 $d_j(u)$ 中的一个，为了方便起见，记 $w_k=x_{j+k}$，$k=1,\cdots,p$. 我们有

$$H_1w_kz_i=H_1w_{k+1},$$

这里指标取模 p. 因而

$$w_kz_i=y_kw_{k+1},$$

这里 $y_k\in H_1$. 又

$$w_kuw_k^{-1}=h_k,\quad d_j(u)=h_1\cdots h_p.$$

现在

$$\begin{aligned}w_k(u,z_i)w_k^{-1}&=w_ku^{-1}w_k^{-1}\cdot w_kz_i^{-1}uz_i\cdot w_k^{-1}\\&=h_k^{-1}y_{k-1}^{-1}w_{k-1}uw_{k-1}^{-1}\quad w_{k-1}^{-1}z_iw_k^{-1}\\&=h_k^{-1}y_{k-1}^{-1}h_{k-1}\quad y_{k-1}\\&=h_k^{-1}h_{k-1}(h_{k-1},y_{k-1})。\end{aligned}$$

但是 $y_i\in H_1$，$h_i\in H$，而且由于 $(H_1,H)\subseteq H_0$，所以我们有

$$w_k(u,z_i)w_k^{-1}\equiv h_k^{-1}h_{k-1}(\mathrm{mod}\,H_0).$$

但是 P 在 P_1 里是正规的，因而 $(u,z_i)\in P$，所以对于 $u_1=(u,z_i)$，$d(u_1)$ 中从傍系 $Hw_k(k=1,\cdots,p)$ 取的对角因子等于 $h_k^{-1}h_{k-1}(\mathrm{mod}\,H_0)$，$k=1,\cdots,p$. 因而根据 $w_kuw_k^{-1}\equiv h_k(\mathrm{mod}\ H_0)$，$k=1,\cdots,p$，我们得出 $w_k(u,z_i)w_k^{-1}\equiv h_k^{-1}h_{k-1}(\mathrm{mod}\ H_0)$，$k=1,\cdots,p$. 现在当 $u=u_0$ 时有 $u_1=(u,z_i)$，$u_2=(u_1,z_i)$，而且有递归等式 $u_{s+1}=(u_s,z_i)$. 我们已经看到，如果

$$w_k u_s w_k^{-1} \equiv h_{k,s} (\mathrm{mod}\, H_0), \quad k = 1, \cdots, p,$$

则

$$w_k u_{s+1} w_k^{-1} \equiv h_{k-1,s} h_{k,s}^{-1} \equiv h_{k,s+1} (\mathrm{mod}\, H_0).$$

因此对 s 施行归纳法，我们得出

$$w_k u_s w_k^{-1} \equiv h_{k-s} h_{k-s+1}^{-s} h_{k-s+2}^{\binom{s}{2}} \cdots h_k^{(-1)^s},$$

这里方次数是正负交替的二项式系数. 根据二项式系数的性质和 $H^p \subseteq H_0$ 的事实，我们有

$$W_k u_{p-1} w_k^{-1} \equiv h_1 h_2 \cdots h_p \equiv d_j(u) (\mathrm{mod}\, H_0).$$

因而

$$d_j(u) \equiv w_k(u, \overbrace{z_i, \cdots, z_i}^{p-1}) w_k^{-1} \,(\mathrm{mod}\, H_0),$$

这里 $u \in P$, $z_i \in P_1$. 如果记

$$e_p(u, z_i) = (u, \overbrace{z_i, \cdots, z_i}^{p-1}),$$

则引理 14.4.5 指出，为了得出 H，只要对 H_0 添加属于 H 的形状 $x_{j+k} e_p(u, z_i) x_{j+k}^{-1}$ 的某些元素（对于全体 $u \in P$），即添加 $e_p(u, z_i)$ 的某些对角因子，这里 $i = 1, \cdots, s$ 而且 $u \in P$. 因为这些因子是 H 内阶为 p 的方幂的元素，而且 P 是西罗 p 子群，我们可以用 H 的元素作变形，因而它们属于 P. 这并不被取模 H_0 而改变，因为 H/H_0 是阿贝尔群.

这证明了下列主要定理.

定理 14.4.1（P. 赫尔）. 设 G_1 是有限群，P_1 是它的西罗 p 子群，N_1 是 P_1 的正规化子，H_1 是包含 N_1 的子群. 再设 $G = u_p(G_1)$ 是由 G_1 中阶与 p 互素的元素生成的子群. 令 $H = G \cap H_1$, $N = G \cap N_1$, $P = G \cap P_1$. 那么 $u_p(H_1) = u_p(H)$. 又如果 $u_p(H) \neq H$，则 $H_0 = H^p(H_1, H) u_p(H)$ 是 H 的真子群，而且 H 可以从 H_0 添加元素 $e_p(u, z_i)$ 的属于 H 的某些共轭者而得到，这里 $u \in P$ 而且 $z_i (i = 1, \cdots, s)$ 是 P_1 的元素. 设

$$G_1 = H_1 + H_1t_1P_1 + \cdots + H_1t_sP_1$$

是 G_1 分解成为 H_1 和 P_1 的二重傍系的分解式，再设 $\pi_i(i = 1, \cdots, s)$ 是 P_1 到 H_1 在 $H_1t_iP_1$ 内的傍系上的置换的传递表示. 那么 π_i 的次数不是 1，而且可以取 z_i，使 $\pi_i(z_i)$ 的阶是 p 而且属于 $\pi_i(P_1)$ 的中心.

推论 14.4.2. 如果对于所有 $u, z \in P_1$ 都有 $e_p(u,z) = 1$，则 $u_p(N_1) = N = u_p(G_1) \cap N$ 而且 $G_1/u_p(G_1) = N_1/u_p(N_1)$. 特别当 P_1 的类小于 p 时就出现这种情况.

这里我们取 $H_1 = N_1$，因而 $H = N$.

设 Q_1 是 P_1 的弱闭子群. 那么正如我们曾经指出过的，Q_1 是 P_1 的正规化子 N_1 的正规子群，因而可以取 Q_1 的正规化子作为子群 $H_1 \supseteq N_1$. 于是前面的定理给出一个结果，它是维兰德定理 (Wielandt[3]) 的一种改进.

定理 14.4.2 (赫尔-维兰德). 设 P_1 是 G_1 的西罗子群而且 Q_1 是 P_1 的弱闭子群. 设 N_1 是 P_1 的正规化子而且 H_1 是 Q_1 的正规化子. 那么从下列条件中的任何一个都能得出 $u_p(H_1) = H = u_p(G_1) \cap H_1$，因而 $G_1/u_p(G_1) = H_1/u_p(H_1)$.

1) $e_p(u,z) = 1$ 对于所有 $u \in P_1$ 和所有 $z \in Q_1$.

2) $e_{p-1}(u,z) = 1$ 对于所有 $u, z \in Q_1$.

3) $Q_1 \subseteq Z_{p-1}(P_1)$，后者是 P_1 的递升中心序列的第 $p-1$ 项.

证明. 像在定理 14.4.1 的证明中一样，设 K_i 是从 P_1 到 H_1 在 $H_1t_iP_1$ 内的傍系上的置换表示 π_i 的核. 设 $Q_1 \subseteq K_i$(如果这可能的话). 那么 $H_1t_iQ_1 = H_1t_i$，因而 $t_iQ_1t_i^{-1} \subseteq H_1$. 因此 $t_iQ_1t_i^{-1}$ 是 H_1 的 p 子群，于是就存在 $y \in H_1$，使得 $y^{-1}t_iQ_1t_i^{-1}y \subseteq p_1$，它是 H_1 的西罗 p 子群. 根据 Q_1 的弱闭性，这说明 $y^{-1}t_iQ_1t_i^{-1}y = Q$，因而 $y^{-1}t_i \in H_1$，H_1 是 Q_1 的正规化子，而且还有 $t_i \in H_1$，这是不可能的. 因此 $Q_1 \nsubseteq K_i$. 然后因为 Q_1 是

P_1 的正规子群，所以 Q_1 在 P_1/K_i 内的像是正规子群，因而必定包含它的中心的元素．因此可以在 Q_1 内取元素z_i．这给出第一个条件．在这个条件里，我们看到只要取$u \in P = P_1 \cap G$，但是我们并不预先知道 P_1 的哪个子群是P．从第三个条件可以得出第一个条件，因为如果 $Q_1 \subseteq Z_{p-1}(P_1)$，则 $z \in Z_{p-1}(P_1)$ 而且 $(u, z) \in Z_{p-2}(P_1)$，$(u, z, z) \in Z_{p-s}$，等等，最后

$$e_p(u, z) = (u, \overbrace{z, \cdots, z}^{p-1}) = 1.$$

对于第二个条件，$e_p(u, z) = e_{p-1}(u_1, z)$，这里 $u_1 = (u, z)$，于是对于 $u \in P_1$ 有 $u_1 \in Q_1$，因而从第二个条件也得出第一个条件．

推论 14.4.3. 设 Q_1 是 P_1 的特征子群．如果 Q_1 在 P_1 内不是弱闭的，则就存在另一个西罗子群 P_2，它包含 Q_1，但是 Q_1 不是它的正规子群．这必定是这样的情形：Q_1 满足定理中的条件(1)，(2) 或 (3)，但是 $G_1/u_p(G_1)$ 和 $H_1/u_p(H_1)$ 不同构．

证明. 因为 Q_1 是 P_1 的特征子群，所以 Q_1 是N_1的正规子群．因此 $N_1 \subseteq H_1$，这里 H_1 是 Q_1 的正规化子．如果 Q_1 在 P_1 内不是弱闭的，则对于某个x，$x^{-1}Q_1x \subseteq P_1$，但是 $x^{-1}Q_1x \neq Q_1$．如果 $x^{-1}Q_1x$ 在 P_1 内是正规的，则根据引理 14.3.1，Q_1 和 $x^{-1}Q_1x$ 在 N_1 内彼此共轭，这是不可能的．因此 $x^{-1}Qx$ 在 P_1内但是不是 P_1 的正规子群，所以 Q_1 在 $P_2 = xP_1x^{-1}$ 内但是不是 P_2 的正规子群．如果 Q_1 满足定理中的条件 (1)，(2) 或 (3)，则定理的结论不成立，只是因为 Q_1 在 P_1 内不是弱闭的．

下面的定理比前面的定理稍为简单些．

定理 14.4.3. 设 P 是 G 的西罗 p 子群，G' 是 G 的导出群．那么 $V_{G\to P}(G) \cong P/P \cap G'$．

证明. 因为 $V_{G\to P}(G)$ 是从G 到 p 群 P/P' 的同态，所以阶

与 p 互素的每个元素都被映成单位元素．因为 G 由 P 和对应于其他素数的西罗子群生成，所以 $V(G)=V(P)$．

设

$$G=P+Px_2+\cdots+Px_n.$$

根据引理 14.4.1，对于 $u\in P$，

$$V(u)\equiv\prod_{i\in C_P(u)}x_iu^{r_i}x_i^{-1}\bmod P',$$

$$V(u)\equiv\prod_{i\in C_P(u)}u^{r_i}(u^{r_i},x_i^{-1})\bmod P',$$

而且
$$V(u)\equiv\prod_{i\in C_P(u)}u^{r_i}\equiv u^n\bmod G'.$$

因此，由于 $(n,p)=1$，当 $u\in P$，$u\notin G$ 时有 $V(u)\not\equiv 1\bmod G'$．但是因为 $V(G)$ 是阿贝尔群，所以 $V(G')\equiv 1$，因此 $P\to V_{G\to P}(P)$ 的核恰好是 $P\cap G'$，所以 $V_{G\to P}(G)\cong P/P\cap G'$．

定理 14.4.4（格润的第一个定理）（Grün[1]）．设 P 是 G 的西罗 p 子群．那么 $V_{G\to P}(G)\cong P/P^*$，这里

$$P^*=[P\cap N_{G'}(P)]\bigcup_{z\in G}(P\cap z^{-1}P'z).$$

证明．根据定理 14.4.3，我们已知 $V_{G\to P}(G)\cong P/P\cap G'$．根据构造 P^* 是包含在 $P\cap G'$ 内的子群的并，因而 $P^*\subseteq P\cap G'$．我们必须证明 $P\cap G'\subseteq P^*$．我们对 u 的阶施行归纳法，来证明 $P\cap G'$ 的每个元素 u 都在 P^* 内．这时显然有 $1\in P^*$．

设

$$G=P+Py_2P+\cdots+Py_sP$$

是用 P 的二重傍系表出的 G 的分解式．设 $u\in P\cap G'$．那么根据引理 14.4.1，

$$V(u)\equiv\prod_{i\in C_P(u)}x_iu^{r_i}x_i^{-1}\bmod P'.$$

这时 $V(u)$ 中从二重傍系 PyP 取的乘积有形状

$$w = \prod_k y v_k u^{r_k} v_k^{-1} y^{-1},$$

这里 $v_1 = 1$ 而且 $v_k \in P$. 又当 P 在 PyP 内有 p^t 个左傍系时有 $\sum_k r_k = p^t$. 在讨论乘积 w 时，我们区别两种情形：情形 1，在 p^t 中有 $t \geqslant 1$；情形 2，$t = 0$，$p^t = 1$.

情形 1. 我们有

$$w \equiv y u^{p^t} y^{-1} \pmod{y P' y^{-1}}.$$

又对于 $v_1 = 1$，我们有一个因子 $y u^{p^b} y^{-1} \in P$，而且因为 $b \subseteq t$，所以我们有 $y u^{p^t} y^{-1} \in P$. 但是还有 $w \in P$，所以

$$w \equiv y u^{p^t} y^{-1} \pmod{P \cap y P' y^{-1}},$$

因而更有

$$w \equiv y u^{p^t} y^{-1} \pmod{P^*}.$$

因为 $u \in P \cap G'$，所以 $V(u) \equiv 1 \pmod{P'}$，因而 $V(y u^{p^t} y^{-1}) \equiv 1 \pmod{P'}$. 于是因为 $y u^{p^t} y^{-1}$ 属于 P，它在 $P \cap G'$ 的核内，而且因为 $t > 1$，它的阶比 u 低，因而根据归纳假设，$y u^{p^t} y^{-1} \in P^*$. 又因为根据归纳假设，$u^{p^t} \in P^*$，所以

$$w \equiv y u^{p^t} y^{-1} \equiv 1 \equiv u^{p^t} \pmod{P^*}.$$

情形 2. 这时 $PyP = Py$，因此 $Py \subseteq N_G(P)$. 又

$$w \equiv y u y^{-1} \equiv u[N_{G'}(P)],$$

而且

$$w \equiv u[\operatorname{mod} P \cap N_{G'}(P)],$$

因而更有 $w \equiv u \pmod{P^*}$. 因此当 w_i 是从包含 P 的 p^{t_i} 个左傍系 Py_iP 取的乘积时，在所有各种情形都有

$$w_i \equiv u^{p^{t_i}} \pmod{P^*}.$$

因此

$$V(u) \equiv u^n \pmod{P^*},$$

这里 $n = [G:P]$ 与 p 互素. 然而对于 $u \in P \cap G'$ 有 $V(u) \equiv 1$，所以 $V(u) \in P' \subseteq P^*$. 因此 $u^n \equiv 1 \pmod{P^*}$，所以 $u \in P^*$，这是我们希望证明的.

定理 14.4.5（格润的第二个定理） 设G是p正规的，H是G的西罗p子群D的中心Z的正规化子．再设$G'(p)$是使$G/G'(p)$为阿贝尔p群的G的最小子群，$H'(p)$是使$H/H'(p)$为阿贝尔群的H的最小子群．那么$G/G'(p)\cong H/H'(p)$.

证明. 设P是G的西罗p子群，Z是它的中心．设$G'(p)\supseteq G'$是使$G/G'(p)$为阿贝尔p群的G的最小子群．那么$G=G'(p)\cup P$，因为$G'(P)$的阶必定被G的阶的不包含p的方幂的约数整除．如果$G^*=P\cup G'$，则$G'(p)\cup G^*=G$．又$G^*\cap G'(p)=G'$，因为G^*/G'只包含阶为p的方幂的元素而且$G'(p)/G'$只包含阶与p互素的元素．根据定理 2.4.1，$G/G'(p)=G^*/G'=P/P\cap G'$．设$N$是$P$的正规化子，$H$是$Z$的正规化子．因为$Z$是$P$的特征子群，所以$H\supseteq N$．现在如果$H'(p)$是使$H/H'(p)$成为阿贝尔$p$群的$H$的最小子群，则像$G$的情形一样，$H/H'(p)=P/P\cap H'$．因此为了证明定理，必须证明$P\cap G'=P\cap H'$．显然$G\supseteq H$，$G'\supseteq H'$，而且$P\cap G'\supseteq P\cap H'$．因而我们需要证明$P\cap H'\supseteq P\cap G'$．根据格润的第一个定理，

$$P\cap G'=(P\cap N')\bigcup_{x\in G}(P\cap x^{-1}P'x).$$

因为$H\supseteq N$所以$P\cap H'\supseteq P\cap N'$．我们还要证明，对于每个$x\in G$，都有

$$P\cap H'\supseteq P\cap x^{-1}P'x.$$

记$M=P\cap x^{-1}P'x$．于是$Z\subseteq N_G(M)$而且$x^{-1}Zx\subseteq N_G(M)$；因为$x^{-1}Zx$是$x^{-1}Px$的中心．这时Z在$N_G(M)$的西罗子群R内，而且$x^{-1}Zx$在$N_G(M)$的西罗子群S内．因此，对于某个$y\in N_G(M)$，Z和$y^{-1}x^{-1}Zxy$同时在G的包含R的同一个西罗子群Q内．根据p正规性，Z和$y^{-1}x^{-1}Zxy$都是Q的中心，因而彼此相等．即$Z=y^{-1}x^{-1}Zxy$，所以$xy=h\in N_G(M)=H$.

但是 $y \in N_G(M)$，因而

$$M = y^{-1}My = y^{-1}Py \cap y^{-1}x^{-1}P'xy$$
$$= y^{-1}Py \cap h^{-1}P'h \subseteq H'.$$

因此 $M = P \cap x^{-1}P'x \subseteq P \cap H'$，定理也就证明了.

P.赫尔的定理也产生格润的第二个定理的改进，从其中消除了“阿贝尔”的要求.

定理 14.4.6（赫尔-格润）. 如果 G 是 p 正规的，则 G 中本身是 p 群的最大商群同构于关于西罗 p 子群的中心的正规化子的同样商群.

证明. 在定理 14.4.2 中取 G_1 为 G，取 P_1 是西罗 p 子群，取 Q_1 为 P_1 的中心，而且取 H_1 为 Q_1 的正规化子. 那么我们看到，G_1 的 p 正规性说明 Q_1 在 P_1 内是弱闭的. 这时因为 $Q_1 = Z(P_1)$，第三个条件成立，因而我们得出 $G_1/u_p(G_1) \cong H_1/u_p(H_1)$. 这些都是极大的 p 商群，于是定理证明了.

我们还可以改进伯恩赛德定理. 在什么情况下群 G 的西罗 p 子群 P 同构于 G 的商群？这就是说，什么时候 $G/u_p(G) = P$？假定这情形成立，记 $B = u_p(G)$；那么 B 由 G 中阶与 p 互素的全体元素组成. 这时 $B \cap P = 1$，$B \cup P = BP = G$. 如果 Q 是 P 的任何子群，则 $B \cup Q = BQ$ 是包含 Q 和阶与 p 互素的全体元素的子群. 这时 B 在 BQ 内是正规的. 记 $W = N_{BQ}(Q)$. 那么 $W \cap B$ 由 W 中阶与 p 互素的元素组成. 明显地，$W \cap B \lhd W$ 而且当然有 $Q \lhd W$. 于是 $W = (W \cap B) \times Q$. 因此属于 Q 的正规化子的每个阶与 p 互素的元素也属于 Q 的中心化子. 我们来证明，$G/u_p(G) \cong P$ 的这个必要条件也是充分的，这就推广了定理 14.3.1.

定理 14.4.7. 群 G 具有商群 $G/u_p(G)$ 同构于西罗 p 子群 P，必要而且只要，对于 P 的每个子群 Q，属于 Q 的正规化子的每个阶与 p 互素的元素也属于 Q 的中心化子.

证明. 我们对于G的阶施行归纳法. 当 $G = P$ 时结论显然成立. 我们先来证明G是 p 正规的. 设Z是P的中心. 根据定理 14.4.2 的推论,如果G不是 p 正规的,则Z包含在另一个西罗 p 子群 P_2 内,但是Z在 P_2 内不是正规的. 于是根据定理 4.2.5, 存在P的子群 Q, 它的正规化包含阶与 p 互素的元素,这元素不属于它的中心化子.根据假设,这不能出现.因而G必定是 p 正规的. 根据定理 14.4.6, $G/u_p(G) \cong H/u_p(H)$, 这里H是Z的正规化子. 如果H是G的真子群, 则根据归纳假设, $H/u_p(H) \cong P$, 定理证明了.

因此我们可以假定 $G = H$, 于是Z在G内是正规的. 但是如果 G/Z 包含 p 群 Q/Z, 它的正规化包含阶与 p 互素的元素,而这元素不属于它的中心化子,则这对于它的逆像Q也成立. 因而我们的假设对 G/Z 成立,所以 G/Z 具有正规子群 K/Z, 使得对应的商群同构于 P/Z. 因为K包含在Z的正规化子内, 而且 K/Z 的阶与 p 互素, 所以K也包含在Z的中心化子内, 因而 $K = Z \times K_1$, 这里 K_1 的阶与 p 互素. 但是 $K_1 = u_p(K) = u_p(G)$ 专门由阶与 p 互素的元素组成. 因此 $G/u_p(G) = P$, 这就是要求证明的.

第十五章　群的扩张和群的上同调

15.1.　正规子群和商群的合成

一般地说，包含已知群U的任何群G都叫做U的扩张。白尔（Baer[11]）详细地研究了一般的群的扩张，然而我们在这里只探讨U是G的正规子群的情形。

施赖尔（Schreier [1,2]）最先考虑构造所有这样的群G的问题，G具有已知的正规子群N和已知的商群$H \cong G/N$。至少总存在一个这样的群，因为N和H的直积就具有这个性质。

我们先假定给了这样的群G，我们仔细地来研究它。设商群$H \cong G/N$的元素记做$1, u, v, \cdots, w$。H的每个元素x对应于N在G内的一个傍系。设对应于x的傍系$\bar{x}N$在G内的代表是$\bar{x}$，而且约定用G的单位元素1作为N的代表。于是

$$G = N + \bar{u}N + \bar{v}N + \cdots + \bar{w}N, \qquad (15.1.1)$$

而且同态$G \to H$使得

$$\bar{u} \to u,\ \bar{u} \in G,\ u \in H. \qquad (15.1.2)$$

于是对于所有$a \in N$，映射

$$a \rightleftarrows \bar{u}^{-1} a \bar{u} = a^u \qquad (15.1.3)$$

是N的自同构，因为N是正规子群。又因为在从G到H上的同态下，$\bar{u} \to u$，$\bar{v} \to v$，所以

$$\bar{u} \cdot \bar{v} = \overline{uv}(u, v), \qquad (15.1.4)$$

这里$(u, v) \in N$。由(15.1.4)给定的所有元素(u, v)的集合

我们叫做因子组，于是在G的构造中出现下列四个已知条件:

1) 正规子群N.

2) 商群H.

3) N的自同构: $a \rightleftarrows a^u$, $a \in N$, $u \in H$.

4) 由$(u, v) \in N$组成的因子组,这里$u, v \in H$.

必须强调的是,一般地说,由(15.1.3)和(15.1.4)定出的自同构和因子组依赖于与u对应的傍系$\bar{u}N$的代表$\bar{u}$的选取.

自同构和因子组必须满足某些条件. 用(15.1.4)两边作元素$a \in N$的变形,我们得出

$$(a^u)^v = (u,v)^{-1}(a^{uv})(u,v). \tag{15.1.5}$$

又因为在G内$(\bar{u}\bar{v})\bar{w} = \bar{u}(\bar{v}\bar{w})$, 由于

$$(\bar{u}\bar{v})\bar{w} = [\overline{uv}(u, v)]\bar{w} = \overline{uv}\bar{w}(u, v)^w$$
$$= \overline{uvw}(uv, w)(u, v)^w,$$

而且

$$\bar{u}(\bar{v}\bar{w}) = \bar{u}[\overline{vw}(v, w)] = \overline{uvw}(u, vw)(v, w),$$

因而

$$(uv,w)(u,v)^w = (u,vw)(v,w). \tag{15.1.6}$$

对于G的两个元素$\bar{u}a$和$\bar{v}b$的乘积,我们有

$$(\bar{u}a)(\bar{v}b) = \bar{u}\bar{v}a^vb = \overline{uv}(u, v)a^vb$$

即

$$(\bar{u}a)(\bar{v}b) = \overline{uv}(u,v)a^vb. \tag{15.1.7}$$

从取1作为N在G内的代表的规定得出,根据(15.1.4), 对于所有$u, v \in H$, 都有

$$(u, 1) = 1 = (1, v). \tag{15.1.8}$$

反之,关于自同构和因子组的条件(15.1.5)和(15.1.6)是具有正规子群N而且$G/N \cong H$的群G存在的充分条件. 取符号$\bar{u}a$, $u \in H$, $a \in N$, 组成体系G, 在G中用下列规则定义

二元乘积运算：

$$\bar{u}a \cdot \bar{v}b = \overline{uv}(u,v)a^v b. \qquad (15.1.9)$$

这个乘积是可结合的，因为

$$\begin{aligned}(\bar{u}a \cdot \bar{v}b) \cdot \bar{w}c &= \overline{uv}(u,v)a^v b \cdot \bar{w}c \\ &= \overline{uvw}(uv, w)(u, v)^w (a^v)^w b^w c \\ &= \overline{uvw}(uv, w)(u, v)^w (v, w)^{-1} a^{vw}(v, w) b^w c \\ &\qquad\qquad [\text{根据 } (15.1.5)] \\ &= \overline{uvw}(u, vw) a^{vw}(v, w) b^w c \quad [\text{根据}(15.1.6)] \\ &= \bar{u}a \cdot \overline{vw}(v,w) b^w c = \bar{u}a \cdot (\bar{v}b \cdot \bar{w}c).\end{aligned}$$

为了反面推导的方便（读者可以自己证明这并非必须），在 (15.1.5) 和 (15.1.6)两个等式之外，不妨假定作为 (15.1.8) 的特殊情形的下列等式成立：

$$(1, 1) = 1. \qquad (15.1.10)$$

如果在 (15.1.5) 中令 $u = v = 1$ 而且利用 (15.1.10)，则我们得出 $(a^1)^1 = a^1$，而且由于 $a^1 = c$ 可以是N的任意元素，我们对于所有 $c \in N$ 都有 $c^1 = c$. 在 (15.1.6) 中令 $u = v = 1$. 那么$1 = (1,1)^w = (1, w)$. 同理，从 $v = w = 1$ 得出 $(u, 1) = 1$. 于是 $\bar{1}1 \cdot \bar{w}c = \bar{w}(1,w)c = \bar{w}c$而且$\bar{u}a \cdot \bar{1}1 = \bar{u}(u,1)a = \bar{u}a$，因而 $\bar{1}1$ 是体系G的单位元素. 因为 $a \rightleftarrows a^w$ 是N的自同构，所以存在N的元素 d，使得对于已知的 $c \in N$ 和 $w \in H$，有 $d^w = (w^{-1},w)^{-1}c^{-1}$. 因此，对于 G 的任意 $\bar{w}c$，我们有 $\overline{w^{-1}}d \cdot \bar{w}c = \bar{1}(w^{-1},w)d^w c = \bar{1}1$. 因为$G$的每个元素都有左逆，这就足以证明$G$是群. 乘法规则 (15.1.9) 使映射

$$\bar{u}a \to u \qquad (15.1.11)$$

是从G到H上的同态，这时核由元素 $\bar{1}a$ 组成. 因为

$$\bar{1}a \cdot \bar{1}b = \bar{1}(1,1)ab = \bar{1}ab,$$

所以 $\bar{1}a \rightleftarrows a$ 是使这个核与N等同的同构. 又因为 $\bar{u}1 \cdot \bar{1}a = \bar{u}(u,1)a = \bar{u}a$，所以可以取 $\bar{u} = \bar{u}1$ 作为N的傍系代表，而且

我们可以把 $\bar{u}a$ 看作 $\bar{u}$ 和 a 的乘积.

我们把这些结果总结成一个定理.

定理 15.1.1 (施赖尔). 给了具有正规子群 N 和商群 $H=G/N$ 的群 G. 如果选取傍系代表 $\bar{u}$, 这里 $\bar{u}N\to u\in H$, 而且取 $\bar{1}=1$, 则就决定满足下列条件的自同构和因子组:

$$(a^u)^v=(u,v)^{-1}(a^{uv})(u,v),\quad a,(u,v)\in N;\quad u,v\in H;$$
$$(uv,w)(u,v)^w=(u,vw)(v,w);\quad (1,1)=1.$$

反之, 如果对于每个 $u\in H$, 给定 N 的自同构 $a\rightleftarrows a^u$, 而且对于这些自同构和因子组 $[(u,v)\in N](u,v\in H)$, 上述条件成立, 则元素 $\bar{u}a(u\in H,\ a\in N)$ 连同乘法规则

$$\bar{u}a\cdot\bar{v}b=\overline{uv}(u,v)a^v b$$

决定具有正规子群 N 和商群 $G/N\cong H$ 的群 G.

如果略去 $(1,1)=1$ 的要求, 则取 $\bar{1}(1,1)^{-1}$ 作为 G 的单位元素时定理仍然成立.

由 $N,H,a\rightleftarrows a^u$ 和因子组 (u,v) 决定的唯一扩张 G 将记做 $E[N,H,a^u,(u,v)]$.

如果更换 N 在 G 内的傍系代表, 取

$$\bar{\bar{u}}=\bar{u}\alpha(u),\quad u\in H,\quad \alpha(u)\in N,\qquad (15.1.12)$$

而且规定 $\bar{\bar{1}}=\bar{1}=1$, 即 $\alpha(1)=1$, 则自同构就更换成

$$a\rightleftarrows a^{u^1}=\bar{\bar{u}}^{-1}a\bar{\bar{u}}=\alpha(u)^{-1}a^u\alpha(u),\qquad (15.1.13)$$

而因子组 (u,v) 更换成因子组 $(u,v)^1$, 使得

$$\bar{\bar{u}}\cdot\bar{\bar{v}}=\bar{u}\alpha(u)\bar{v}\alpha(v)=\overline{uv}(u,v)\alpha(u)^v\alpha(v)$$
$$=\overline{\overline{uv}}(u,v)^1=\overline{uv}\alpha(u,v)(u,v)^1.\qquad (15.1.14)$$

定义. 两个扩张 $E_1=E[N,H,a^u,(u,v)]$ 和 $E_2=E[N,H,a^{u^1},(u,v)^1]$ 是等价的, 假如在自同构和因子组之间有关系

$$a^{u^1}=\alpha(u)^{-1}a^u\alpha(u),$$
$$(u,v)^1=\alpha(uv)^{-1}(u,v)\alpha(u)^v\alpha(v),$$

这里 $\alpha(u)$ 是元素 u 的在 N 内取值的函数，而且 $\alpha(1)=1$.
我们记做

$$E[N,H,a^u,(u,v)] \sim E[N,H,a^{u^1},(u,v)^1].$$

E_2 与 E_1 的等价性取决于更换同一个群 G 内子群 N 的傍系代表，因而它显然是对称的、自反的和传递的真等价关系。

如果 N 在 G 内的傍系代表 $\bar{u}$ 能取成使

$$\overline{\overline{uv}} = \bar{\bar{u}}\,\bar{\bar{v}}, \qquad (15.1.15)$$

即 $(u,v)^1=1$，则傍系代表组成同构于 H 的群，可以把它与 H 等同起来. 如果这种情形出现，则我们说 G 是 N 的可裂扩张，或说 G 是 N 和 H 的半直积.

定理 15.1.2. $G=E[N,H,a^u,(u,v)]$ 是 N 的可裂扩张，必要而且只要存在函数 $\alpha(u)\in N$, $u\in H$，使得对于所有 $u,v\in H$，都有

$$(u,v)\alpha(u)^v\alpha(v)=\alpha(uv).$$

证明. 如果所取的傍系代表使 $G=E[N,H,a^u,(u,v)]$ 成为 N 的可裂扩张，则 $(u,v)^1=1$，而且当取 $\bar{\bar{u}}=\bar{u}\alpha(u)$ 时，就有

$$(u,v)\alpha(u)^v\alpha(v)=\alpha(uv). \qquad (15.1.16)$$

反之，如果函数 $\alpha(u)$ 存在，使得 (15.1.16) 成立，则用条件 $a^{u^1}=\alpha(u)^{-1}a^u\alpha(u)$ 决定对应于 $\bar{\bar{u}}=\bar{u}\alpha(u)$ 的自同构 a^{u^1}. 于是 $E[N,H,a^{u^1},(u,v)^1]=G$ 存在，而且等价于对所有 $u,v\in H$ 都有 $(u,v)^1=1$ 的扩张，因而 G 是 N 的可裂扩张.

15.2. 中心扩张

假定在群 A 借助于群 H 的扩张中，所有的因子 (u,v) 都属于 A 的中心 B. 那么我们说 $E[A,H,a^u,(u,v)]$ 是 A 借助于 H 的中心扩张. 例如如果 A 是阿贝尔群，则 $B=A$，因而

A 的所有扩张都是中心扩张。

对于中心扩张，(15.1.5) 简化成

$$(a^u)^v = a^{uv}, \tag{15.2.1}$$

这说明 A 的自同构 $a \rightleftarrows a^u$ 组成一个群，它是 H 的同态像. 设 χ 表示从 H 到 A 的自同构群的同态. 再有，如果傍系代表 $\bar{u}$ 由属于 B 的因子 $\alpha(u)$ 来更换，则自同构不变. 因此，对于白尔叫做 H-χ 扩张 (Baer[1]) 的这种扩张，自同构是固定的而且组成一个群，它是 H 的同态像. 对于中心扩张，这就取消了条件 (15.1.5)，而只需要考虑 (15.1.6)，它现在成为

$$(uv, w)(u, v)^w = (u, vw)(v, w). \tag{15.2.2}$$

这时对于等价的扩张有

$$(u, v)^1 = \alpha(uv)^{-1}(u, v)\alpha(u)^v\alpha(v), \tag{15.2.3}$$

这里 $\alpha(u) \in B$.

如果因子组 $(u,v)_1$ 和 $(u, v)_2$ 都满足 (15.2.2) 而且定义

$$(u, v)_3 = (u, v)_1(u, v)_2 \quad \text{对于所有 } u, v \in H, \tag{15.2.4}$$

则元素 $(u,v)_3$ 也满足 (15.2.2)，而且组成决定 A 的 H-χ 扩张的因子组. 在因子组乘积的这个定义下，存在着单位元素，即所有 $(u, v) = 1$ 的因子组，还存在逆，即把 (u, v) 换成 $(u,v)^{-1}$ 的因子组. 再有，对于等价的因子组，如果 $(u,v)_1^* \sim (u, v)_1$ 和 $(u, v)_2^* \sim (u, v)_2$，则 $(u, v)_1^*(u, v)_2^* \sim (u, v)_1 \cdot (u, v)_2$. 因此全体 H-χ 因子组的集合是一个阿贝尔群，即使把等价的因子组等同起来也是如此. 把等价的因子组等同起来而得到的群叫做**扩张群**.

设 H 是有限的，我们定义

$$f(v) = \prod_u (u, v). \tag{15.2.5}$$

(15.2.2) 对于所有的 $u \in H$ 乘起来，我们得出

$$f(w)f(v)^w = f(vw)(v, w)^n, \qquad (15.2.6)$$

这里 n 是 H 的阶. 与 (15.2.3) 比较,

$$(v, w)^n \sim 1. \qquad (15.2.7)$$

又如果 m 是 B 的所有元素的阶的倍数,则因为 $(u, v) \in B$, 所以

$$(v, w)^m = 1. \qquad (15.2.8)$$

因此下列定理成立.

定理 15.2.1. 扩张群的任意元素的阶整除 H 的阶和 B 的元素的阶的最小公倍数.

推论 15.2.1. 如果 m 和 n 是互素的,则 A 的所有 H-χ 扩张都等价于 A 和 H 的半直积.

作为这个定理的应用, 我们来证明关于并未假定为中心扩张的扩张的定理 15.2.2.

定理 15.2.2. 设 mn 阶有限群 G 包含 m 阶正规子群 K 而且具有 n 阶的商群 $H = G/K$, 这里 m 和 n 是互素的. 那么 G 是 K 的可裂扩张.

证明. 只要证明 G 具有 n 阶的子群. 我们对 m 施行归纳法,当 $m = 1$ 时定理是显然的. 设 $m > 1$ 而且 p 是整除 m 的素数. G 中对应于 p 的所有西罗子群 S_p 是 K 的子群,因为 K 至少包含一个西罗子群 S_p, 而且 K 是正规的, 因而 S_p 的共轭者也属于 K. 因此 G 内的西罗 p 子群 S_p 的个数与 K 内的个数相同. 因此根据定理 1.6.1, $[G:N_G(S_p)] = [K:N_K(S_p)]$, 因而 $[N_G(S_p):N_K(S_p)] = [G:K] = n$, $N_G(S_p)$ 和 $N_K(S_p)$ 分别是 S_p 在 G 和 K 内的正规化子. 这时当然有 $N_K(S_p) = N_G(S_p) \cap K$, 因而根据定理 2.4.1, $N_k(S_p)$ 是 $N_G(S_p)$ 的正规子群. 如果 $N_G(S_p)$ 是 G 的真子群, 则根据归纳假设, 它包含 n 阶的子群.

因此可以假定 $G = N_G(S_p)$, 于是 $K = N_K(S_p)$. 如果 S_p

是K的真子群，则根据归纳假设，G包含阶为$[G:S_p]$而且同构于G/S_p的子群，因而包含同构于G/K的n阶子群，这就证明了定理．因此问题归结为$K=S_p$的情形．这时如果S_p是阿贝尔群，则G是S_p的中心扩张，因而根据定理15.2.1的推论，G是S_p的可裂扩张，证明了定理．如果S_p不是阿贝尔群，则S_p的中心Z是S_p的真子群，而且是S_p的特征子群，它必定是G的正规子群．因此，根据归纳假设，G/Z包含n阶子群U/Z．于是Z在G的对应子群U内是正规的而且有指数n，因而根据归纳假设，U包含n阶子群，这就对最后这种情形证明了定理．

15.3. 循环扩张

假设H是由元素x生成的m阶的有限循环群；H的元素是

$$1, x, x^2, \cdots, x^{m-1}. \tag{15.3.1}$$

设$G/N=H$，取$\bar{x}$作为映成x的N的傍系代表，还可以取$\bar{x}^2, \cdots, \bar{x}^{m-1}$作为分别映成$x^2, \cdots, x^{m-1}$的$N$的傍系代表，因而

$$G=N+N\bar{x}+\cdots+N\bar{x}^{m-1}. \tag{15.3.2}$$

这时

$$\bar{x}^m=\alpha, \tag{15.3.3}$$

这里α是N的元素．

于是对于N的自同构$a\rightleftarrows a^x$，必定有

$$a^{x^m}=\alpha^{-1}a\alpha, \quad \alpha\in N. \tag{15.3.4}$$

其次从恒等式

$$\bar{x}^{-1}\bar{x}^m\bar{x}=\bar{x}^m. \tag{15.3.5}$$

得出

$$\alpha^k = \alpha. \tag{15.3.6}$$

我们来证明，(15.3.4) 和 (15.3.6) 完全决定了N借助于H的扩张．

定理 15.3.1. 设H是m阶的有限循环群．那么群N借助于H的扩张G存在，必要而且只要存在N的自同构 $a \rightleftarrows a^x$ 和元素$\alpha \in N$，使得(1)这自同构的m次方幂是由α作变形而得出的N的内自同构，而且(2)α在这自同构下不变．

证明．我们已经证明，如果扩张存在，则自同构 $a \rightleftarrows a^x$ 和元素α满足 (15.3.4) 和 (15.3.6)．反之，我们来证明 (15.3.4) 和 (15.3.6) 足以决定一个扩张．H的元素是 1，x，$\cdots$，x^{m-1}，或 x^i，$0 \leqslant i = m-1$．我们按下列方式定义自同构和因子组：

$$a^{x^0} = a, \quad a^{x^i} = (a^{x^{i-1}})^x, \quad i = 1, \cdots, m-2, \tag{15.3.7}$$

$$(x^i, x^j) = 1, \quad 如果 i + j \leqslant m - 1, \tag{15.3.8.1}$$

$$(x^i, x^j) = \alpha, \quad 如果 m \leqslant i + j. \tag{15.3.8.2}$$

利用这些定义我们容易验证 (15.1.5) 和 (15.1.6) 满足，因而根据定理 15.1.1，决定了一个扩张．

如果H是无限阶的循环群，我们可以令$(i, j) = 1$对于所有i和j都成立，而且我们发现自同构 $a \rightleftarrows a^x$ 不必加以限制．这说明 $x^i = x^{-i}$ 对于所有i都成立．

15.4. 定义关系和扩张

在上一节内我们看到，当H是循环群时，扩张一个群N的条件特别简单．它就对应于H的特别简单的定义关系．在本节中将要谈到，对于更一般的群H，扩张条件如何依赖于定义关系．

设群G由生成元素$x, y, z, \cdots$和定义关系

$$\phi_i(x, y, z, \cdots) = j, \quad i = 1, 2, \cdots, r \qquad (15.4.1)$$

给定．我们可以假定H的每个元素h由生成元素和它们的逆组成的确定的字$h = h(x, y, z, \cdots)$表出．于是如果G是N借助于H的扩张，则我们可以取由$\bar{x}, \bar{y}, \bar{z}, \cdots$组成的对应的字作为$N$的傍系代表，使得在同态$G \to H$下有

$$\bar{x} \to x, \quad h(\bar{x}, \bar{y}, \cdots) \to h(x, y, \cdots). \qquad (15.4.2)$$

现在设F_1是具有对应于x, y, z的生成元素$\mathbf{x}, \mathbf{y}, \mathbf{z}$的自由群．那么我们有由

$$\begin{aligned} &\mathbf{x} \to \bar{x} \to x, \\ &\mathbf{y} \to \bar{y} \to y, \\ &\cdots\cdots\cdots \end{aligned} \qquad (15.4.3)$$

决定的同态

$$F_1 \to \bar{H} \to H, \qquad (15.4.4)$$

这里$\bar{H}$是G中由$\bar{x}, \bar{y}, \bar{z}, \cdots$生成的子群，因而它至少包含$N$的每个傍系的一个元素．因此$G = \bar{H} \cup N$．于是如果$F_2$是以$N$作为同态像的自由群，则我们可以取自由群$F = F_1 \cup F_2$而且定义同态

$$\begin{aligned} &F \to G \to H, \quad F = F_1 \cup F_2, \\ &F_1 \to \bar{H} \to H, \quad F_2 \to N \to 1. \end{aligned} \qquad (15.4.5)$$

$\bar{H}$的每个元素$\bar{h}$以变形的方式导出N的自同构

$$\bar{h}^{-1} a \bar{h} = a^h, \quad \bar{h} \in \bar{H}, a \in N. \qquad (15.4.6)$$

在映射$F_1 \to H$下，我们有$H = F_1/W$，这里W是包含$\phi_i(\mathbf{x}, \mathbf{y}, \cdots)$的最小正规子群．因此在$\bar{H} \to H$下我们有$\phi_i(\bar{x}, \bar{y}, \cdots) \to 1$．于是

$$\phi_i(\bar{x}, \bar{y}, \cdots) = \alpha_i \in N. \qquad (15.4.7)$$

在自由群F内有恒等式

$$u_1 u_2 \cdots u_r = z_1 z_2 \cdots z_s,$$

假如这些 u 和这些 z 是这样的字，它们的乘积的简化形式相同．在从 F 到 G 上的映射下，任何恒等式仍然成立．特别地 W 和 F_2 将被映射到 N 内．因此，从关于由 W 和 F_2 生成的不变子群中的字的恒等式，利用 (15.4.6) 和 (15.4.7)，导出关于 α_i 和自同构 $a \rightleftarrows a^h$ 的条件，它们可以解释为存在 N 借助于 H 的扩张 G 的条件．因为 $\overline{uv}^{-1}\overline{u}\overline{v}$ 属于 $N\cap\overline{H}$，它是 W 的元素在 G 内的像，即是 $\phi_i(\bar{x}, \bar{y}, \cdots) = \alpha_i$ 的共轭者的乘积．因此每个因子 $(u, v) = \overline{uv}^{-1}\overline{u}\overline{v}$ 都是 W 的元素在 $\overline{H}$ 内的像，而且如果 $\bar{u} = h_1(\bar{x}, \bar{y}, \cdots)$，$\bar{v} = h_2(\bar{x}, \bar{y}, \cdots)$，$\overline{uv} = h_3(\bar{x}, \bar{y}, \cdots)$，则 (u, v) 是 W 的元素

$$h_3(\mathbf{x}, \mathbf{y}, \cdots)^{-1}h_1(\mathbf{x}, \mathbf{y}, \cdots)h_2(\mathbf{x}, \mathbf{y}, \cdots) \quad (15.4.8)$$

的像．

定理 15.1.1 的条件是 F 内的恒等式，它可以按规则 (15.4.6) 和 (15.4.7) 而解释成关于自同构和因子组的条件．例如恒等式

$$\bar{v}^{-1}(\bar{u}^{-1}a\bar{u})\bar{v} = (\overline{uv}^{-1}\bar{u}\bar{v})^{-1}(\overline{uv}^{-1}a\overline{uv})(\overline{uv}^{-1}\bar{u}\bar{v}), \quad (15.4.9)$$

利用关于自同构的 (15.4.6) 而且把 W 的元素换成 N 的元素，就是关系式 (15.1.5)

$$(a^u)^v = (u,v)^{-1}(a^{uv})(u,v).$$

同理，恒等式

$$(\overline{uvw}^{-1}\overline{uv}\bar{w})\bar{w}^{-1}(\overline{uv}^{-1}\bar{u}\bar{v})\bar{w} = (\overline{uvw}^{-1}\bar{u}\overline{vw})(\overline{vw}^{-1}\bar{v}\bar{w}) \quad (15.4.10)$$

就是关系式 (15.1.6)

$$(uv, w)(u, v)^w = (u, vw)(v, w).$$

因而 N 借助于 H 的扩张存在的条件可以解释成 F 内的恒等式．注意 N 的定义关系不会在这些条件中出现．这些条件可以看作是用来求得与 H 的定义关系协调的 N 的元素 α_i 和 N

的自同构的已知条件．当H是阿贝尔群时这些条件变成当然成立，因为这时总可以取代表使$\overline{uv}=\bar{u}\bar{v}$而且使因子都是单位元素，其次只需要自同构组成一个群.

在实用上可能难以决定导出扩张的存在条件的F的恒等式．在下一节里我们将对于N借助于H的中心扩张来决定它们.

15.5. 群环和中心扩张[1]

考虑具有中心C的群N借助于有限群H的中心扩张．像在§15.2中那样，假定自同构满足

$$(a^u)^v=a^{uv}, \tag{15.5.1}$$

我们假定了所有的因子$(u,v)=\overline{uv}^{-1}\bar{u}\bar{v}$都属于$C$．根据引理7.2.2(对于右傍系而不是左傍系)，这些元素生成$\bar{H}$的子群T使得$\bar{H}/T=H$．而如果

$$\phi_i(x,y,\cdots)=1 \tag{15.5.2}$$

是H的定义关系，则

$$\phi_i(\bar{x},\bar{y},\cdots)=\alpha_i\in C, \tag{15.5.3}$$

因为α_i当然属于T，而且由C中的元素生成.

如果r和s是C的自同态，则可以按下列规则定义自同态$r+s$:

$$a^ra^s=a^{r+s}. \tag{15.5.4}$$

因此，根据(15.5.1)和(15.5.4)，H的群环H^*是C的算子环．这时群环H^*由下列元素组成:

$$c_1h_1+\cdots+c_nh_n, \tag{15.5.5}$$

这里$h_1,\cdots,h_n$是H的元素而$c_1,\cdots,c_n$是整数．H^*的元

---

1) 参看 M. Hall [1].

素相加是对应系数相加. H^* 中的乘法由 H 中的乘法 $h_ih_g = h_k$ 连同两个分配律决定. 容易验证 H^* 是结合环,而且 H 的单位元素就是 H^* 的单位元素.

我们把具有算子环 H^* 的阿贝尔群 A 叫做**算子自由的**,假如它具有这样的基底 $a_1, a_2, \cdots, a_r$, 使得 A 的任何元素有唯一的表示式

$$a = a_1^{z_1}a_2^{z_2}\cdots a_r^{z_r}, \quad z_i \in H^*. \tag{15.5.6}$$

因而从 $a = 1$ 得出 $z_1 = z_2 = \cdots = z_r = 0$.

定理 15.5.1. **算子自由的群 A 借助于有限群 H 的唯一的扩张是 A 与 H 的半直积.**

证明. 在 A 内每个元素 b 有唯一的表示式

$$b = a_1^{z_1}\cdots a_r^{z_r}, \quad z_i \in H^*.$$

设 $z_i = c_{i1}h_1 + \cdots + c_{in}h_n, \quad i = 1, \cdots, r$, 令

$$(b; h_j) = a_1^{c_{1j}}a_2^{c_{2j}}\cdots a_r^{c_{rj}}.$$

因而当 $t = h_1, h_2, \cdots, h_n$ 时, b 有唯一的表示

$$b = \prod_t (b; t)^t, \quad t = h_1, \cdots, h_n. \tag{15.5.7}$$

因此对于因子组有

$$(u, v) = \prod_t (u, v; t)^t, \tag{15.5.8}$$

而且根据 (15.5.7) 的唯一性, (15.1.6) 变成

$$(uv, w; t)(u, v; tw^{-1}) = (u, vw; t)(v, w; t). \tag{15.5.9}$$

于是如果令 $\bar{\bar{u}} = \bar{u}\prod_t (u, t^{-1}; 1)^{-t}$ 对于所有 $u \in H$, 则我们可以利用 (15.5.9) 通过直接计算而验证

$$\bar{\bar{u}}\bar{\bar{v}} = \overline{\overline{uv}}. \tag{15.5.10}$$

因此新的代表组成一个群,所以 G 是 A 和 H 的半直积.

根据 §15.4 的结果, 群 N 借助于群 H 的中心扩张的条件

是 (15.5.1) 和下列条件

$$\prod_i \alpha_i^{u_i} = 1, \quad u_x \in H^*, \qquad (15.5.11)$$

这里像在 (15.5.3) 里一样，$\phi_i(\bar{x}, \bar{y}, \cdots) = \alpha_i$. 现在假定$N$是算子自由的群。 我们知道这时 $\alpha_i = 1 (i = 1, \cdots, r)$ 是 (15.5.11) 的解，而且所有其他的解可以从更换傍系代表而得出. 如果令 $\bar{x} = \xi\bar{\bar{x}}, \bar{y} = \eta\bar{\bar{y}}, \cdots$, 则 $\phi_i(\xi\bar{\bar{x}}, \eta\bar{\bar{y}}, \cdots) = 1$, 这时利用等式

$$\alpha\bar{\bar{z}} = \bar{\bar{z}}\alpha^z, \alpha \in N, \qquad (15.5.12)$$

我们得到

$$1 = \phi_i(\xi\bar{\bar{x}}, \eta\bar{\bar{y}}, \cdots) = \phi_i(\bar{\bar{x}}, \bar{\bar{y}}, \cdots)\xi^{x_i}\eta^{y_i}\cdots. \qquad (15.5.13)$$

因此 $\alpha_i^{-1} = \xi^{x_i}\eta^{y_i}\cdots$必定也满足条件 (15.5.11)，因为这些值是在半直积中更换傍系代表而得到的. 取 $\xi, \eta, \cdots$ 作为 N 的无关的基元素，我们得到在 H^* 中成立的下列关系:

$$\sum_i x_i u_i = 0, \ \sum_i y_i u_i = 0, \cdots, i = 1, \cdots, r. \qquad (15.5.14)$$

H^* 的元素 $x_i, y_i, \cdots$可以从定义H的关系 $\phi_i(x, y, \cdots) = 1$ 利用等式 (15.5.12) 决定. 因此，(15.5.11) 中的 u_i 限于 H^* 中满足 (15.5.14) 的量. 如果我们能证明逆命题: 满足条件(15.5.14) 的u_i 使 (15.5.11) 成立，则就可以把决定条件 (15.5.11) 的问题简化成解方程 (15.5.14) 的问题. 为了证明这个事实，我们利用马格努斯(Magnus[2])的方法.

定理 15.5.2. 给了群H和N. 存在 N 借助于 H 的扩张的条件是: (1) 对应于H的元素 h 的自同构 $a \rightleftarrows a^h$ 满足条件 (15.5.1); (2) 存在N的中心 C 的元素 α_i, 使得 $\phi_i(\bar{\bar{x}}, \bar{\bar{y}}, \cdots) = \alpha_i, i = 1, \cdots, r$, 这里 $\phi_i(x, y, \cdots) = 1$ 是H的定义关系; (3) α_i 具有性质 (15.5.11), 其中 u_i 是 H^* 中满足

(15.5.14）的元素.

证明. 前面的讨论证明了定理中的各部分，唯一未证的是满足(15.5.14)的每一组 u_i 都具有性质 (15.5.11).

考虑由 $\mathbf{x}$, $\mathbf{y}$, $\cdots$ 生成的自由群 F_1（像在§15.4中一样），设 $H = F_1/W$，这里 W 是包含 $\phi_i(\mathbf{x}, \mathbf{y}, \cdots)$ 的最小正规子群. 设 W' 是 W 的导出群. 那么作为 W 的特征子群的 W' 是 F_1 的正规子群. 于是 $T = F_1/W'$ 是具有下列性质的群: (1) T 由 $x, y, \cdots$ 生成，(2) T 具有正规子群 $V = W/W'$，使得 $T/V = H$; (3) V 是阿贝尔群. 最后,明显地,具有这些性质的任何群都是 T 的同态像,因为任何这种群必定是 F_1 的这样的同态像,在这同态下 W' 的元素都映成单位元素. 我们利用一个引理来证明定理，这个引理的证明留到定理的证明之后.

引理 15.5.1. 给了矩阵$\begin{pmatrix} h, & 0 \\ L, & 1 \end{pmatrix}$,这里 $h \in H$, L 是若干个未知数的系数属于 H^* 的线性齐式,它们按下列规则相乘:

$$\begin{pmatrix} h_1, & 0 \\ L_1, & 1 \end{pmatrix}\begin{pmatrix} h_2, & 0 \\ L_2, & 1 \end{pmatrix} = \begin{pmatrix} h_1h_2, & 0 \\ L_1h_2 + L_2, & 1 \end{pmatrix}.$$

那么对应于 $x, y, \cdots$，我们有矩阵 $\bar{x} = \begin{pmatrix} x, & 0 \\ t_x, & 1 \end{pmatrix}$, $\cdots$，而且这些矩阵生成同构于 $T = F_1/W'$ 的群.

注意因为矩阵$\begin{pmatrix} 1, & 0 \\ L, & 1 \end{pmatrix}$生成加法群(即是阿贝尔群),所以这个群总是 T 的同态像.

在中心扩张里 $\bar{H}$ 是 T 的同态像. 因此,如果关系式

$$\phi_i(\bar{x}, \bar{y}, \cdots)^{u_i} = 1, \quad u_i \in H^* \qquad (15.5.15)$$

在 T 内成立,则对应的等式 (15.5.11) 必定在 $\bar{H}$ 内成立.

假定引理成立. 那么在 T 内有子群 V 的下列元素:

$$\phi_i(\bar{x}, \bar{y}, \cdots) = \begin{pmatrix} 1, & 0 \\ L_i, & 1 \end{pmatrix}, \quad i = 1, \cdots, r, \qquad (15.5.16)$$

这里 L_i 是系数从 H^* 取的 $t_x, t_y, \cdots$ 的线性齐式. 我们把下列元素添加到 V:

$$\xi = \begin{pmatrix} 1, & 0 \\ t_\xi, & 1 \end{pmatrix}, \quad \eta = \begin{pmatrix} 1, & 0 \\ t_\eta, & 1 \end{pmatrix}, \cdots, \qquad (15.5.17)$$

这里 $t_\xi, t_\eta, \cdots$ 是新的未知数. 对于前面采用的$\bar{u}(u \in H)$,

$$\bar{u}^{-1}\xi u = \begin{pmatrix} 1, & 0 \\ t_\xi u, & 1 \end{pmatrix}. \qquad (15.5.18)$$

因此, 在把 (15.5.17) 中的元素添加到V时,我们添加了一个算子自由的群. 再有,

$$\xi \bar{x} = \begin{pmatrix} x, & 0 \\ t_\xi x + t_x, & 1 \end{pmatrix}. \qquad (15.5.19)$$

因此我们得到把 (15.5.16) 的 L_i 中的 t_x 换成 $t_\xi x + t_x$ 的 $\phi_i(\xi\bar{x}, \eta\bar{y}, \cdots)$,等等. 因此根据

$$\phi_i(\xi\bar{x}, \eta\bar{y}, \cdots) = \phi_i(\bar{x}, \bar{y}, \cdots)\xi^{x_i}\eta^{y_i}\cdots \qquad (15.5.20)$$

和 L_i 的线性性质,我们有

$$\xi^{x_i}\eta^{y_i}\cdots = \begin{pmatrix} 1, & 0 \\ L_i(t_\xi x), & 1 \end{pmatrix}. \qquad (15.5.21)$$

所以如果等式 (15.5.14) 成立,则

$$\sum_i L_i(t_\xi x)u_i = 0. \qquad (15.5.22)$$

这时因为 t_ξ 是不满足任何关系的未知数,由此得出

$$\sum_i L_i u_i = 0 \qquad (15.5.23)$$

对于 L_i 的任何的元都成立. 把这应用到(15.5.16),我们得出

$$\prod_i \phi_i(\bar{x}, \bar{y}, \cdots)^{u_i} = 1. \qquad (15.5.24)$$

因为这个关系在 T 内成立, 它在 $\bar{H}$ 内也成立, 所以我们证明了,当 (15.5.14) 成立时, 在 $\bar{H}$ 内有 $\prod_i \alpha_i^{u_i} = 1$. 因此(15.5.11)是 (15.5.14) 的推论, 这就完成了定理的证明, 剩下的是证明

上述引理.

引理的证明. 设在商群$H = F_1/W$中这样地取W的傍系代表,使得它们对于F_1的元素的字典排列而说是最前的. 于是同样的字典排列也可以带到H内，而且如果$h = h(\mathbf{x}, \mathbf{y}, \cdots)$是傍系$Wh$的最前元素,则取$h = h(x, y, \cdots) \in H$作为$h$的字典排列式的典范形式. 因此,同一个字可以用来表示H的元素和W的对应的傍系代表,而且可以把H的元素的典范形式的长度叫做这元素的长度. 现在考虑映射

$$\bar{x} \to \begin{pmatrix} x, & 0 \\ t_x, & 1 \end{pmatrix}, \bar{y} \to \begin{pmatrix} y, & 0 \\ t_y, & 1 \end{pmatrix}, \cdots,$$

这里$x, y, \cdots$是H的生成元素而且矩阵的合成规则是

$$\begin{pmatrix} h_1, & 0 \\ L_1, & 1 \end{pmatrix}\begin{pmatrix} h_2, & 0 \\ L_2, & 1 \end{pmatrix} = \begin{pmatrix} h_1h_2, & 0 \\ L_1h_2 + L_2, & 1 \end{pmatrix},$$

这里$h_1, h_2 \in H$, L_1, L_2是系数从H^*取的$t_x, t_y, \cdots$的线性齐式. 前面说过,由这些矩阵生成的群K总是T的同态像,因为$\begin{pmatrix} h, & 0 \\ L, & 1 \end{pmatrix} \to h$显然是从$K$到$H$的同态. 而且这个同态的核由元素$\begin{pmatrix} 1, & 0 \\ L, & 1 \end{pmatrix}$组成,它是加法阿贝尔群.

根据定理 7.3.6, W是F_1的自由子群,它具有自由生成元素c_{ij}:

$$c_{ij} = \mathbf{h}_i\mathbf{x}\mathbf{h}_j^{-1} \neq 1, \quad \mathbf{h}_j = \phi(\mathbf{h}_i\mathbf{x}), \qquad (15.5.25)$$

这里$\mathbf{x}$是F_1的生成元素.

其次，根据引理 7.2.3. 字$\mathbf{h}_i$不会以$\mathbf{x}^{-1}$结尾,字$\mathbf{h}_i$不会以$\mathbf{x}$结尾. 群W'由元素c_{ij}的所有换位子生成，而群W/W'是以c_{ij}取模W'作为基底的自由阿贝尔群. 由此得出K是$T = F_1/W'$的一一的表示，只要我们能证明对应于$\bar{h}_i\bar{x}\bar{h}_j^{-1}$的元素$c_{ij}$在$K$内是无关的. 在映射$F_1 \to H$下有$c_{ij} \to 1$, $\mathbf{h}_i \to h_i$, $\mathbf{h}_j \to h_j$和$\mathbf{x} \to x$, 因而在H内有$h_ix = h_j$. 现在设

$$\bar{h}_i \to \begin{pmatrix} h_i, & 0 \\ L(h_i), & 1 \end{pmatrix}, \quad \bar{x} \to \begin{pmatrix} x, & 0 \\ t_x, & 1 \end{pmatrix},$$

$$\bar{h}_j \to \begin{pmatrix} h_j, & 0 \\ L(h_j), & 1 \end{pmatrix}.$$

那么

$$\bar{c}_{ij} \to \begin{pmatrix} h_i x h_j^{-1}, & 0 \\ L(h_i)xh_j^{-1} + t_x h_j^{-1} - L(h_j)h_j^{-1}, & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1, & 0 \\ L(h_i)h_i^{-1} + t_x h_j^{-1} - L(h_j)h_j^{-1}, & 1 \end{pmatrix}^{1)}, \quad (15.5.26)$$

因为在H内 $h_i x = h_j$.

我们必须详细地探讨一下在对应于元素 $\bar{h}_i$ 的矩阵中出现的线性齐式 $L(h_i)$. 设

$$\bar{x} \to \begin{pmatrix} x, & 0 \\ t_x, & 1 \end{pmatrix}, \quad \bar{x}^{-1} \to \begin{pmatrix} x^{-1}, & 0 \\ -t_x x^{-1}, & 1 \end{pmatrix}.$$

令 $q(a) = t_a$ 如果 $a = x$ 是生成元素，又令 $q(a) = -t_{a^{-1}}a$ 如果 $a^{-1} = x$ 是生成元素. 如果 $\bar{h} = a_1 a_2 \cdots a_r$ 是任意的字，其中每个 a_i 是 $\bar{x}, \bar{y}, \cdots$ 或 $\bar{x}^{-1}, \bar{y}^{-1}, \cdots$ 中的一个，则我们有

$$\bar{h} \to \begin{pmatrix} h, & 0 \\ L(h), & 1 \end{pmatrix},$$

其中

$$L(h) = q(a_1)a_2 \cdots a_r + q(a_2)a_3 \cdots a_r + \cdots + q(a_{r-1})a_r + q(a_r), \quad (15.5.27)$$

这里 $h = a_1 a_2 \cdots a_r$.

对 r 施行归纳法而且利用矩阵的相乘规则，容易证明这个公式. 我们看到从 (15.5.27) 能得出下列恒等式:

---

1) 原书有错.——译者

$$L(h)h^{-1} = q(a_1)a_1^{-1} + q(a_2)a_2^{-1}a_1^{-1} + \cdots + q(a_r)a_r^{-1}a_{r-1}^{-1}\cdots a_1^{-1}. \qquad (15.5.28)$$

如果 h 由典范形式表出，则 $q(a_i)$ 乘上 $a_1a_2\cdots a_i$ 的逆，后者根据W的代表的许赖尔性质也是典范形式. 因而作为群环H^*的基底，适宜于采用H的元素的典范形式的逆.

对于W的每个生成元素 c_{ij}，存在唯一的 h_j 和 x. 因此可以取 $t_xh_j^{-1}$ 对应于 c_{ij}. 这个 $t_xh_j^{-1}$ 可以这样决定，h_j 具有典范形式，而 h_jx^{-1} 则是简化字而不是典范形式，因为它等于典范形式 h_i. 但是在 (15.5.26) 中，线性齐式 $L(h_i)h_i^{-1} + t_xh_j^{-1} - L(h_j)h_j^{-1}$ 不包含其他这种类型的项. 事实上，根据 (15.5.25)，在 $L(h_i)h_i^{-1}$ 或 $L(h_j)h_j^{-1}$ 中出现的其他加项有形状 $q(a_k)a_k^{-1}\cdots a_1^{-1}$，这里 $a_1\cdots a_k$ 是 h_i 或 h_j 的最前一段，因而根据关于 h 的施赖尔条件，它本身是具有典范形式的一个 h. 这时如果 $a_k = y$ 是生成元素，则 $q(a_k)a_k^{-1}\cdots a_1^{-1} = t_yy^{-1}\cdots a_1^{-1} = t_yh^{-1}$，这里 h 以 y 结尾，因而 hy^{-1} 不是简化字. 而如果 $a_k = y^{-1}$，这里 y 是生成元素，则 $q(a_k)a_k^{-1}\cdots a_1^{-1} = -ty \cdot a_{h-1}^{-1}\cdots a_1^{-1} = -tyh^{-1}$，这里 $hy^{-1} = a_1\cdots a_k$ 具有典范形式. 因而 $t_xh_j^{-1}$ 是在对应于 $\bar{c}_{ij}$ 的线性齐式中唯一的这种类型的项，并且不同的 $\bar{c}_{ij}$ 对应于不同的项. 因此线性齐式 $L(c_{ij})$ 是线性无关的，而且 c_{ij} 生成自由阿贝尔群，它当然同构于 W/W'. 因此，由对应于 $\bar{x}, \bar{y}, \cdots$ 的矩阵生成的群K是 $T = F_1/W'$ 的确切的表示，引理也就证明了.

15.6. 二 重 模

设Ω是任意乘法群而且A是**二重Ω模**，即是满足下列条件的加法阿贝尔群:

1) A 以 Ω 作为左右两边算子的群，使得对于给定的

$a \in A$ 和 $\xi \in \Omega$, ξa 和 $a\xi$ 是 A 的唯一决定的元素.

2) 分配性

$$\xi(a_1 + a_2) = \xi a_1 + \xi a_2,$$
$$(a_1 + a_2)\xi = a_1\xi + a_2\xi,$$

因而

$$-\xi a = \xi(-a), \quad -a\xi = (-a)\xi,$$
$$\xi 0 = 0\xi = 0.$$

3) $1a = a1 = a$, 这里 1 是 Ω 的单位元素.

4) 结合性

$$\xi(\eta a) = (\xi\eta)a,\ (\xi a)\eta = \xi(a\eta) \text{ 和 } (a\xi)\eta = a(\xi\eta).$$

这些定律对于所有 $a_1, a_2, a \in A$ 和所有 $\xi, \eta \in \Omega$ 都成立.

实质上,二重 Ω 模就是这样的加法阿贝尔群,它以 $\Omega \times \Omega$ 的元素 (ξ,η) 作为可分配的算子.

在应用中常常出现 Ω 在一边(例如左边,是恒同地作用的,这是说对于所有 $\xi \in \Omega$ 和 $a \in A$ 都有 $\xi a = a$. 在这种情形下,我们简单地略去左边算子,而且把它说成单边的模.

举例说,设 A 是群 G 的正规的阿贝尔子群而且记 $\Omega = G/A$. 如果 $\xi = Au_\xi$, 则 $u_\xi^{-1}au_\xi$ 只取决于 a 和 ξ, 而不依赖于 u_ξ 在傍系中的选取. 因而可以记 $u_\xi^{-1}au_\xi = a^\xi$ 而不致引起误会. 这就是单边模的例子, 只不过 A 是用乘法表出的. 在展开上同调的一般定理时, 用加法记号表出 A 是特别方便的.

15.7. 上链,上边缘和上同调群[1)]

给了二重 Ω 模 A, 我们定义 $C^n = C^n(A,\Omega)$ 为 n 个变量的所有函数组成的加法群,这 n 个变量独立地在 Ω 内取值,函

---

1) 参看 Eilenberg and MacLane [1,2] 以及 MacLane [2].

数值在A内取，而且满足条件：如果至少有一个$\xi_i = 1$，则

$$f(\xi_1, \cdots, \xi_n) = 0. \tag{15.7.1}$$

C^n 的元素叫做n维上链. 根据定义 $C^0 = A$，而零维上链根本就是A的任意元素.

上边缘算子δ是指从 C^n 到 C^{n+1} 的下列映射:

$$\begin{aligned}(\delta f)(\xi_0, \xi_1, \cdots, \xi_n) &= \xi_0 f(\xi_1, \cdots, \xi_n) \\ &+ \sum_{t=1}^{n}(-1)^t f(\xi_0, \xi_1, \cdots, \xi_{t-2}, \xi_{t-1}\xi_t, \xi_{t+1}, \cdots, \xi_n) \\ &+ (-1)^{n+1} f(\xi_0, \xi_1, \cdots, \xi_{n-1})\xi_n.\end{aligned} \tag{15.7.2}$$

这里$f \in C^n$，而且容易验证 $\delta f \in C^{n+1}$. 映射 $f \to \delta f$ 对于加法说是同态. 在群论中特别有用的是 $n = 0, 1, 2$ 的情形. 这时上边缘公式是

$$\begin{aligned}(\delta f)(\xi) &= \xi f - f\xi = \xi a - a\xi, \text{因为 } f = a \in A, \\ (\delta f)(\xi, \eta) &= \xi f(\eta) - f(\xi\eta) + f(\xi)\eta, \\ (\delta f)(\xi, \eta, \zeta) &= \xi f(\eta, \zeta) - f(\xi\eta, \zeta) + f(\xi, \eta\zeta) \\ &\quad - f(\xi, \eta)\zeta.\end{aligned} \tag{15.7.3}$$

定理 15.7.1. 如果f是任意上链，则$\delta^2 f = 0$.

证明. 取n使$f \in C^{n-2}$. 那么 $\delta f \in C^{n-1}$. 因此，当我们根据定义用δf的值来表示$(\delta^2 f)(\xi_1, \xi_2, \cdots, \xi_n)$时，我们得到正负交替的$n+1$项:

$$u_0 - u_1 + u_2 - \cdots + (-1)^n u_n.$$

这里每个u_i在用f的值表出时是正负交替的n项，我们可以写成:

$$\begin{aligned}u_i = u_{i0} - u_{i1} + \cdots + (-1)^{i-1}u_{i,i-1} \\ + (-1)^i u_{i,i+1} + \cdots + (-1)^{i+j-1}u_{i,i+j} + \cdots.\end{aligned}$$

因此

$$\delta^2 f(\xi_1, \cdots, \xi_n) = \sum_{i<j}(-1)^{i+j-1}u_{ij} + \sum_{i>j}(-1)^{i+j}u_{ij},$$

这里 i 和 j 取 1 到 n 的值．然而容易验证，对于所有 i 和 j 都有 $u_{ij}=u_{ji}$．因此上述等式的右边等于零．

如果 $f\in C^n$ 有条件 $\delta f=0$，则 f 叫做 n 维上圈[1]，这些上圈组成由 δ 导出的从 C^n 到 C^{n+1} 的同态的核 $Z^n=Z^n(A,\Omega)$．

如果 $f\in C^n$ 而且存在元素 $g\in C^{n-1}$ 使得 $\delta g=f$，则 f 叫做 n 维上边缘．这些上边缘组成 C^{n-1} 在映射 δ 下的像．$B^n=B^n(A,\Omega)$．我们定义 $B^0=0$．

根据定理 15.7.1，每个上边缘都是上圈，因而对于所有 n，$B^n\subseteq Z^n$．商群 Z^n/B^n 叫做二重 Ω 模 A 的 n 维上同调群．我们把它记做

$$H^n(A,\Omega)=Z^n/B^n.$$

在上链 $f(\xi_1,\cdots,\xi_n)$ 的定义中，我们用 (15.7.1) 限定在有一个或更多的元是单位元素时上链取零值．在很多情形里这种限制是能满足的，例如在应用到前面提到过的因子组时就是如此．我们把这种上链叫做正规化的．当 (15.7.1) 这个限制被略去时，我们说成未正规化的上链． 定理 15.7.1 当然对于两种情形都成立，因为在证明时并未用到 (15.7.1)． 它们的区别是为了某种便利，因为我们可以证明，关于未正规化的上链的各维上同调群都同构于关于正规化的上链的对应的上同调群．

定理 15.7.2. 关于未正规化的上链的 n 维上同调群 $H^n(A,\Omega)$ 同构于关于正规化的对应的上同调群．

证明． 我们把 n 维正规化的上链、上边缘和上圈分别记做 C^n，B^n 和 Z^n，而且在未正规化的情形使用记号 C'^n，B'^n 和 Z'^n．

对于 $n=0$ 和 $n=1$，容易验证 $B^0=B'^0=0$，$Z^0=Z'^0$

1）也叫上循环．——译者

和 $B^1 = B'^1$, $Z^1 = Z'^1$, 因而 $H^0(A, \Omega)$ 和 $H^1(A, \Omega)$ 在这两种情形里都相等. 这时主要的验算是: 如果 $f(\xi) \in Z'^1$, 则 $\xi f(\eta) - f(\xi\eta) + f(\xi)\eta = 0$, 因而在取 $\xi = \eta = 1$ 时有 $f(1) = 0$, 因而 $f(\xi)$ 是正规化的,即 $Z'^1 = Z^1$.

现在假定 $n > 1$. 显然有 $B^n \subseteq B'^n$ 和 $Z^n \subseteq Z'^n$. 因此关于 C^n 的上同调类,即 B^n 在 C^n 内的傍系,对应于关于 C'^n 的唯一的同调类, 即 B'^n 的包含它的傍系. 这个对应当然是从 $H^n(A, \Omega)$ 到 $H'^n(A, \Omega)$ 的同态. 为了证明它是同构,需要证明它是一一的,这就要用到两个引理. 当两个上链的差是上边缘时, 我们说这两个上链是上同调的. 因而两个上圈上同调,必要而且只要它们属于同一个上同调类.

引理 15.7.1. 每个未正规化的上圈总上同调于一个正规化的上圈.

引理 15.7.2. 如果某个上链的上边缘是正规化的, 则它是正规化的上链的上边缘.

引理的证明. 我们说上链 $f(x_1, \cdots, x_n)$ 是 i 正规化的, $i = 0, \cdots, n$, 假如当前 i 个元中有一个是单位元素时它取零值. 因而 0 正规化的上链是 C'^n 的未正规化的上链, 而 n 正规化的上链是 C^n 的正规化的上链. 对于 $f(x_1, \cdots, x_n)$,我们令 $f = f_0$ 而且逆归地定义

$$f_{i+1} = f_i - \delta g_{i+1}, i = 0, \cdots, n-1, \qquad (15.7.4)$$

这里

$$g_{i+1}(x_1, \cdots, x_{n-1}) = (-1)^i f_i(x_1, \cdots, x_i, 1, x_{i+1}, \cdots, x_{n-1}). \qquad (15.7.5)$$

我们看到 $f = f_0$ 和 f_n 相差一个上边缘,又因为 $\delta f_i = \delta f_{i+1}$, 所以 $f = f_0, f_1, \cdots, f_n$ 具有相同的上边缘 δf.

引理 15.7.3. 如果 δf 是正规化的,则 f_i 是 i 正规化的.

用这个引理可以证明前两个引理. 事实上, 对于引理

15.7.1，如果 f 是未正规化的上圈，则 $\delta f = 0$，即 δf 显然是正规化的上链，因而上同调于 $f_0 = f$ 的 f_n 是正规化的上圈． 对于引理 15.7.2，如果 $g = \delta f$ 是上边缘而且 g 是正规化的，$g \in C^{n+1}$，则 $g = \delta f_0 = \cdots = \delta f_n$，这里 f_n 是正规化的．

我们对 i 施行归纳法来证明引理 15.7.3，引理在 $i = 0$ 时显然成立．假设引理对于 i 成立，考虑 $i+1$ 的情形，这时需要证明

$$f_{i+1}(x_1, \cdots, x_i, 1, x_{i+2}, \cdots, x_n) = 0. \qquad (15.7.6)$$

根据 (15.7.4) 中 f_{i+1} 的定义，我们有

$$\begin{aligned}
&f_{i+1}(x_1, \cdots, x_i, 1, x_{i+2}, \cdots, x_n)\\
&\quad = f_i(x_1, \cdots, x_i, 1, x_{i+2}, \cdots, x_n)\\
&\qquad - x_1 g_{i+1}(x_2, \cdots, x_i, 1, x_{i+2}, \cdots, x_n)\\
&\qquad + \sum_{j=1}^{i-1}(-1)^{j-1} g_{i+1}(x_1, \cdots, x_j x_{j+1}, \cdots, x_i, 1, x_{i+2}, \cdots, x_n)\\
&\qquad + (-1)^{i-1} g_{i+1}(x_1, \cdots, x_{i-1}, x_i \cdot 1, x_{i+2}, \cdots, x_n)\\
&\qquad + (-1)^{i} g_{i+1}(x_1, \cdots, x_i, 1 \cdot x_{i+2}, \cdots, x_n)\\
&\qquad + \sum_{j=i+2}^{n-1}(-1)^{j-1} g_{i+1}(x_1, \cdots, x_i, 1, x_{i+2}, \cdots, x_j x_{j+1}, \cdots, x_n)\\
&\qquad + (-1)^n g_{i+1}(x_1, \cdots, x_i, 1, x_{i+2}, \cdots, x_{n-1}) x_n. \qquad (15.7.7)
\end{aligned}$$

利用 (15.7.5)，因为根据归纳假设 f_i 是 i 正规化的，所以 g_{i+1} 是 i 正规化的． 这说明在 (15.7.7) 中，包含 x_1 在左边的项和 $j = 1$ 到 $i - 1$ 的和式中的各项都是零．接着的两项互相消去．现在对于留下的项用 (15.7.5) 换去 g_{i+1}．这就给出

$$\begin{aligned}
&f_{i+1}(x_1, \cdots, x_i, 1, x_{i+2}, \cdots, x_n)\\
&\quad = f_i(x_1, \cdots, x_i, 1, x_{i+2}, \cdots, x_n)\\
&\qquad + \sum_{j=i+2}^{n-1}(-1)^{i+j-1} f_i(x_1, \cdots, x_i, 1, 1, x_{i+2}, \cdots, x_j x_{j+1}, \cdots, x_n)\\
&\qquad + (-1)^{n+i} f_i(x_1, \cdots, x_i, 1, 1, x_{i+2}, \cdots, x_{n-1}) x_n. \quad (15.7.8)
\end{aligned}$$

而根据假设，$\delta f_i = \delta f$ 是未正规化的，因而

$$(-1)^{i+1}\delta f(x_1, \cdots, x_i, 1, 1, x_{i+2}, \cdots, x_n) = 0. \tag{15.7.9}$$

又因为根据归纳假设，f_i是 i 正规化的，(15.7.8) 的右边由(15.7.9)的展开式中所有不是零的项组成．因此

$$f_{i+1}(x_1, \cdots, x_i, 1, x_{i+2}, \cdots, x_n) = 0, \tag{15.7.10}$$

这就用归纳法证明了引理 15.7.3，因而引理 15.7.1 和 15.7.2 也证明了，最后还证明了定理 15.7.2.

15.8. 上同调对扩张理论的应用

设 A 是群 G 的正规阿贝尔子群而且 $\Omega = G/A$ 是商群．如果傍系 $Au_\xi = \xi$ 是 Ω 的元素，则对于 $a \in A$，$u_\xi^{-1}au_\xi$ 只取决于 a 和 ξ 而不依赖于 u_ξ 在傍系中的选取．因此可以记 $u_\xi^{-1}au_\xi = a\xi$ 而不会有误会，在这种记号下，Ω 是作用于 A 的右侧的算子群，而且我们认为 Ω 在左侧是恒同地作用的．设 A 是具有固定算子群 Ω 的加法群，而且对于因子组使用记号 $f(u,v) = (u,v)$，那么 (15.2.2) 变成

$$f(uv,w) + f(u,v)w = f(u,vw) + f(v,w). \tag{15.8.1}$$

移项后我们得出

$$f(v,w) - f(uv,w) + f(u,vw) - f(u,v)w = 0, \tag{15.8.2}$$

因而因子组是二维上圈．根据(15.2.3)．两个因子组 $f(u, v)$ 和 $f_1(u, v)$ 等价的条件是

$$f_1(u, v) = f(u, v) + f(v) - f(uv) + f(u)v, \tag{15.8.3}$$

即 f_1 和 f 相差上边缘 $f(v) - f(uv) + f(u)v$．这里我们说过 Ω 在左侧是恒同地作用的，因此扩张群是二维上同调群

$H^2(A,\Omega)$. 我们把它写成一个定理.

定理 15.8.1. 阿贝尔群 A 借助于群 Ω 的扩张群是二维上同调群 $H^2(A,\Omega)$, 这里:

1) Ω 在左侧是恒同地作用的.

2) Ω 在右侧的作用导出 A 的自同构.

3) 因子组 $f(u,v)$ 是 Z^2 的上圈.

4) 等价的因子组相差 B^2 的上边缘.

在把 G 写成 A 的傍系的和时取单位元素作为 A 的代表就导出正规化性质 $f(1,1)=0$. 在 (15.8.1) 中令 $u=v=1$, 我们得出

$$f(1,w)+f(1,1)w=f(1,w)+f(1,w), \tag{15.8.4}$$

因此

$$f(1,w)=0. \tag{15.8.5}$$

同理, 令 $v=w=1$, 我们得出

$$f(1,1)-f(u,1)+f(u,1)-f(u,1)=0, \tag{15.8.6}$$

因而还有

$$f(u,1)=0, \tag{15.8.7}$$

这说明我们处理的是正规化的上圈.

我们来证明上同调理论的一个普遍定理, 它包含定理 15.2.1 作为特殊情形.

设 Ω 是 m 阶的有限群. 那么对于每个 $n>0$, 我们可以定义加法同态 σ, 它以下列方式把 C^n 映到 C^{n-1}:

$$(\sigma f)(x_2,\cdots,x_n)=\sum_{x\in\Omega}x^{-1}f(x,x_2,\cdots,x_n). \tag{15.8.8}$$

这里 $f\in C^n$, 因而容易验证 $\sigma f\in C^{n-1}$.

记 $g=\sigma f$, 来计算 $(\delta g)(x_1,\cdots,x_n)$:

$$
\begin{aligned}
&(\delta g)(x_1, \cdots, x_n) \\
&\quad = x_1\Sigma x^{-1}f(x, x_2, \cdots, x_n) \\
&\qquad - \Sigma x^{-1}f(x, x_1x_2, \cdots, x_n) \\
&\qquad \cdots\cdots\cdots\cdots\cdots \\
&\qquad + (-1)^{j-1}\Sigma x^{-1}f(x, x_1, \cdots, x_{j-1}, x_j, \cdots, x_n) \\
&\qquad \cdots\cdots\cdots\cdots\cdots \\
&\qquad + (-1)^{n-1}\Sigma x^{-1}f(x, x_1, \cdots, x_{n-1}x_n) \\
&\qquad + (-1)^n[\Sigma x^{-1}f(x, x_1, \cdots, x_{n-1})]x_n. \quad (15.8.9)
\end{aligned}
$$

和号是对所有 $x \in \Omega$ 取的.

再考虑 $(\delta f)(x, x_1, \cdots, x_n)$.

$$
\begin{aligned}
(\delta f)(x, x_1, \cdots, x_n) = &\ xf(x_1, \cdots, x_n) \\
&- f(x \cdot x_1, x_2, \cdots, x_n) \\
&+ f(x, x_1x_2, \cdots, x_n) \\
&\cdots\cdots\cdots\cdots\cdots \\
&+ (-1)^n f(x, x_1, \cdots, x_{n-1}x_n) \\
&+ (-1)^{n+1} f(x, x_1, \cdots, x_{n-1})x_n.
\end{aligned}
\qquad (15.8.10)
$$

然后利用 (15.8.10) 来计算

$$
\begin{aligned}
\sigma(\delta f)(x_1, \cdots, x_n) &= \sum_{x \in \Omega} x^{-1}(\delta f)(x, x_1, \cdots, x_n) \\
&= mf(x_1, \cdots, x_n) \\
&\quad - \Sigma x^{-1}f(xx_1, x_2, \cdots, x_n) \\
&\quad + \Sigma x^{-1}f(x, x_1x_2, \cdots, x_n) \\
&\quad \cdots\cdots\cdots\cdots\cdots \\
&\quad + (-1)^n\Sigma x^{-1}f(x, x_1, \cdots, x_{n-1}x_n) \\
&\quad + (-1)^{n+1}\Sigma x^{-1}f(x, x_1, \cdots, x_{n-1})x_n.
\end{aligned}
\qquad (15.8.11)
$$

在和式 $S = \sum_{x \in \Omega} x^{-1}f(xx_1, x_2, \cdots, x_n)$ 中, 令 $y = xx_1$, 因而

$$S = x_1 \Sigma y^{-1} f(y, x_2, \cdots, x_n) = x_1 \sigma f(x_2, \cdots, x_n),$$

因为 x_1 是 Ω 的固定元素，所以 y 随 x 而遍历整个 Ω. 因此 (15.8.11) 变成

$$\sigma(\delta f) = mf - \delta(\sigma f). \tag{15.8.12}$$

这给出

定理 15.8.2. 如果 $f \in C^n$, 则 $\sigma(\delta f) + \delta(\sigma f) = mf$.

推论 15.8.1. 如果 $f \in Z^n$, 则 $mf \in B^n$.

事实上，$f \in Z^n$ 是说 $\delta f = 0$, 因而 mf 是 σf 的上边缘. 我们的结论是：如果 Ω 的阶是 m, 则上同调群 $H^n = Z^n/B^n$ 的每个元素的阶都整除 m. 定理 15.2.1 是这个结果当 $n = 2$ 时的特殊情形.

关于因子组有伽许兹 (Gaschütz [1]) 的进一步的结果，它的更一般的形式由艾克曼 (Eckmann [1]) 给出. 这个结果是关于一个群 Ω 和它的子群 B 的上同调的. 这时假定 B 在 Ω 内的指数是有限数 m.

$$\Omega = B \cdot 1 + Bs_2 + \cdots + Bs_m, \quad s_1 = 1. \tag{15.8.13}$$

这时如果 $a_1, a_2, \cdots, a_n$ 是 Ω 的元素，则我们记 $\overline{s_i a_1} = s_{i1}$, 这里加杠表示元素所属的傍系的代表. 同理记

$$\overline{s_{i1} a_2} = s_{i2}, \cdots, \overline{s_{i,n-1} a_n} = s_{in}.$$

我们用下列公式定义 $f(a_1, \cdots, a_n) \in C^n$ 的转移 $T(f(a_1, \cdots, a_n))$:

$$T(f(a_1, \cdots, a_n)) = \sum_{i=1}^{m} s_i^{-1} f(s_i a_1 s_{i1}^{-1}, s_{i1} a_2 s_{i2}^{-1}, \cdots, s_{i,n-1} a_n s_{in}^{-1}) s_{in}. \tag{15.8.14}$$

注意总有 $s_{i,j-1} a_j s_{ij}^{-1} \in B$, 因而对于 $f \in C^n(A, \Omega)$, Tf 属于子群 $\Omega C^n(A, B) \Omega$.

定理 15.8.3 (伽许兹定理). 如果 $f(a_1, \cdots, a_n) \in Z^n$ 而且 B 是在 Ω 内有指数 m 的子群，则

$$Tf(a_1, \cdots, a_n) \equiv mf(a_1, \cdots, a_n) \bmod B^n.$$

推论 15.8.2. 转移的上同调类并不依赖于（15.8.13）中傍系代表 s_i 的选取.

定理的证明. 考虑

$$\sum_{i=1}^{m}(\delta f)(s_i^{-1}, s_i a_1 s_{i1}^{-1}, \cdots, s_{i,n-1}a_n s_{in}^{-1})s_{in}$$

$$-\sum_{i=1}^{m}(\delta f)(a_1, s_{i1}^{-1}, s_i, a_2 s_{i2}^{-1}, \cdots, s_{i,n-1}a_n s_{in}^{-1})s_{in}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$+(-1)^{j-1}\sum_{i=1}^{m}(\delta f)(a_1, \cdots, a_{j-1}, s_{i,j-1}^{-1}, s_{i,j-1}a_j s_{ij}^{-1}, \cdots)s_{in}$$

$$+(-1)^{j}\sum_{i=1}^{m}(\delta f)(a_1, \cdots, a_{j-1}, a_j, s_{ij}^{-1}, s_{i,j}a_{j+1}s_{i,j+1}^{-1}, \cdots)s_{in}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$+(-1)^{n}\sum_{i=1}^{m}(\delta f)(a_1, \cdots, a_n, s_{in}^{-1})s_{in} = 0 \qquad (15.8.15)$$

因为 $f \in Z^n$，这和式中每一项都是零，因而 $\delta f = 0$. 展开上式 $n+1$ 行中每一行的上边缘而且对于 δf 的对应项从 $i=1$ 到 m 求和. 这时第一行的第一项给出

$$\Sigma s_i^{-1}f(s_i a_1 s_{i1}^{-1}, \cdots, s_{i,n-1}a_n s_{in}^{-1})s_{in} = Tf(a_1, \cdots, a_n). \qquad (15.8.16)$$

末一行的末一项给出

$$(-1)^n(-1)^{n+1}\Sigma f(a_1, \cdots, a_n)s_{in}^{-1}s_{in} = -mf(a_1, \cdots, a_n). \qquad (15.8.17)$$

因为 $s_{i,j-1}^{-1} \cdot s_{i,j-1}a_j s_{ij}^{-1} = a_j \cdot s_{ij}^{-1}$，所以对于 $j = 1, \cdots, n$，第 j 行和第 $j+1$ 行的第 $j+1$ 项互相消去. 我们现在把第 $j+1$ 行的第 i 项和第 i 行的第 $j+2, \cdots, n+2$ 项放在一起. 这就得出

$$(-1)^j a_1 \sum_{i=1}^{m} f(a_2, \cdots, a_j, s_{ij}^{-1}, s_{ij}a_{i,j+1}s_{i,j+1}^{-1}, \cdots)s_{in},$$

$$+ (-1)^{j+1} \sum_{i=1}^{m} f(a_1a_2, \cdots, a_j, s_{ij}^{-1}, s_{ij}a_{i,j+1}s_{i,j+1}^{-1}, \cdots)s_{in},$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$+ (-1)^{2j} \sum_{i=1}^{m} f(a_1, \cdots, a_{j-1}a_j, s_{ij}^{-1}, s_{ij}a_{i,j+1}s_{i,j+1}^{-1}, \cdots)s_{in},$$

$$+ (-1)^{2j+1} \sum_{i=1}^{m} f(a_1, \cdots, a_{j-1}, s_{i,j-1}^{-1}, s_{i,j-1}a_{ij}s_{ij}^{-1}, \cdots)s_{in},$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$+ (-1)^{n+j+1} \sum_{i=1}^{m} f(a_1, \cdots, a_{j-1}, s_{i,j-1}^{-1}, s_{i,j-1}a_{ij}s_{ij}^{-1}, \cdots)s_{i,n-1}a_n. \tag{15.8.18}$$

而如果对于元 $u_1, \cdots, u_{n-1}$，我们用下列公式定义函数 $F_j(u_1, \cdots, u_{n-1}) \in C^{n-1}$:

$$F_j(u_1, \cdots, u_{n-1})$$
$$= \sum_{i=1}^{m} f(u_1, \cdots, u_{j-1}, \sigma_i^{-1}, \sigma_i u_j \sigma_{ij}^{-1}, \cdots, \sigma_{i,n-1}u_{n-1}\sigma_{in}^{-1})\sigma_{in}, \tag{15.8.19}$$

这里 $\sigma_i = s_i$ 而且递归地有 $\sigma_{it} = \overline{\sigma_{i,t-1}u_t}$，则 (15.8.18) 中各项正好是上边缘 $(-1)^j(\delta F_j)(a_1, \cdots, a_n)$，因为在对 i 求和时，s_{ij} 或 $s_{i,j-1}$ 都可以作为 σ_i。如果 j 遍历从 1 到 n 的值，则上边缘 $(-1)^j(\delta F_j)(a_1, \cdots, a_n)$ 包括了 (15.8.15) 的除已抵消的项以及 (15.8.16) 和 (15.8.17) 的项外的各项。这就证明了定理。

伽许兹定理的群论形式是下列定理：

定理 15.8.4 (伽许兹定理). 设 $F = [(u, v)]$，$u, v \in H$，$(u, v) \in A$，是阿贝尔群 A 借助于有限群 H 的 H-χ 扩张的因子组。设 B 是 H 的指数为 m 的子群，而且

$$H = B \cdot 1 + Bs_2 + \cdots + Bs_m, \quad s_1 = 1.$$

那么

$$(u,v)^m \sim \prod_{i=1}^{m} (s_i u \overline{s_i u}^{-1}, \overline{s_i u} v \overline{s_i uv}^{-1})^{s_i uv}.$$

其中的元 $s_i u \overline{s_i u}^{-1}$ 和 $\overline{s_i u} v \overline{s_i uv}^{-1}$ 当然是 B 的元素.

推论 15.8.3. 如果当 $x, y \in B$ 时有

$$(x, y) = 1, \quad 则\ (u,v)^m \sim 1.$$

这个定理有很多推论，而其中最有用的是连系 A 的 H-χ 扩张和 A 的 $S(p)$-χ 扩张的，这里 $S(p)$ 是 H 的西罗 p 子群. 设 H 的阶是 $n = p^e m$，而 $S(p)$ 的阶是 p^e. 设 $E = E(H)$ 是 A 的 H-χ 扩张的群，就像在 §15.2 里所定义的那样. E 的每个元素是等价的因子组 $F_i = [(u,v)_i]$ 的类. 根据定理 15.2.1，E 的每个元素的阶整除 n. 因而 E 是周期阿贝尔群而且是它的西罗子群 $E(p)$ 的直积.

定理 15.8.5. 设 $E = E(H)$ 是阿贝尔群 A 借助于有限群 H 的 H-χ 扩张的群. 那么 E 的西罗 p 子群 $E(p)$ 同构于群 E_p，E_p 是把 A 的 H-χ 扩张的因子组 $F = [(u,v)]$ 限制成取元 (x,y)，$x, y \in S(p)$，而决定的 $S(p)$-χ 扩张的群，这里 $S(p)$ 是 H 的西罗 p 子群.

证明. 对于 A 的 H-χ 扩张的因子组 $F = [(u,v)]$，我们定义 p 等价

$$(u,v) \underset{p}{\sim} (u,v)_1,$$

假如在限定元 $x, y \in S(p)$ 而导出 $S(p)$-χ 扩张时有

$$(x, y) \sim (x, y)_1.$$

这确实是等价关系. 其次，设 E_1 是 E 的由这种因子组 $F = [(u,v)]$ 组成的子群，对于它在限定 $x, y \in S(p)$ 时，有 $(x, y) \sim 1$. 于是 E 的元素对应于 p 等价的因子组，必要

而且只要它们属于 E_1 的同一个傍系．因此 E/E_1 同构于群 E_p，E_p 是限定因子组 $F=[(u,v)]$ 的元 $x,y\in S(p)$ 而得到的 $S(p)$-χ 扩张的群．根据伽许兹定理的推论，取 $S(p)$ 作为子群 B，E_1 的每个元素的阶都整除 $S(p)$ 的指数 m，又根据定理 15.2.1，E_p 的每个元素的阶都整除 p^e．因为 $(p^e,m)=1$，所以 E_p 和 E 的西罗 p 子群 $E(p)$ 都同构于 E/E_1，因而它们彼此同构，这就证明了定理．

定理 15.8.6. A 的 H-χ 扩张在 A 上可裂，必要而且只要对于整除 H 的阶 n 的每个素数 p，限定于 H 的西罗 p 子群 $S(p)$ 的扩张可裂．

证明． 从 A 借助于 H 的扩张可裂显然得出 A 借助于每个 $S(p)$ 的扩张可裂．我们来证明逆命题．设 $F=[(u,v)]$ 是由 H-χ 扩张决定的因子组．根据假设，$(u,v)\sim(u,v)_1$，这里当 $x,y\in S(p)$ 时有 $(x,y)=1$．根据推论有 $(u,v)^m\sim(u,v)^m\sim 1$，这里 $n=p^e m$．这对于整除 n 的每个 p 都成立．使 $(u,v)^m\sim 1$ 的不同的 m 的最大公约数是1，因而 $(u,v)\sim 1$，所以 A 借助于 H 的扩张可裂．定理证明完毕．

第十六章　群的表示

16.1. 一般注解

我们把从群G到某个群W的任何同态都叫做G的**表示**．特别有价值的是从G到群W的便于计算的表示．例如在第五章里讨论的群G的置换表示，即从G到对称群S_n的同态．

代替作为表示群的对称群，我们转向域F上的向量空间V的自同态．这种一一的自同态组成群，当V在F上的维数是有限数n时，这个群叫做**完全线性群**$L_n(F)$而且可以用F上的非奇异的$n \times n$矩阵来表出．这里我们考虑用线性变换来表示群G．在这种表示下我们可以把G的元素看作V的算子．于是被对应于G的元素的线性变换变到自身的、V的子空间是这表示的不变子空间，又当把V看作以F和G作为算子的加法群时，这些就是容许子群N.

向量空间V的全体自同态的集合是一个环．因此G在V上的线性表示通过加法和系数乘法而导出G在F上的群环R_G的线性表示．同理，V的任何容许子群N也随着G的表示而产生R_G的表示．因此难怪在群环R_G的分解和线性表示的分解之间有着密切的关系．历史上群表示的理论和环的结构理论是各自地发展的，而且只在相当近的年代才在这两种理论之间确定了密切的关系．

16.2. 矩阵表示. 特征标[1]

定义. 群G的n阶矩阵表示是指定义在G上的函数ρ，它在某个域F上的完全线性群$L_n(F)$内取值，使得对于所有x, $y \in G$，都有$\rho(xy) = \rho(x)\rho(y)$.

根据定义$\rho(x)$是非奇异矩阵，而且$x \to \rho(x)$是从G到$L_n(F)$的同态. 这时我们必须有$\rho(1) = I_n$，I_n是$n \times n$单位矩阵，而且$\rho(x^{-1}) = [\rho(x)]^{-1}$，后者是矩阵$\rho(x)$的逆矩阵. 同态$x \to \rho(x)$的核$K$是$G$的正规子群，而且矩阵$\rho(x)$一一地表示了$G/K$. 如果核$K$是1，则这表示是一一的.

定义. 表示ρ的特征标χ是定义在G上的函数:

$$\chi(x) = \mathrm{Tr}\,\rho(x)^{2)}.$$

因此特征标是域K中的数. 如果表示的阶数是1，则$\chi = \rho$.

我们说两个表示ρ和ρ^*等价，假如存在非奇异矩阵$S \in L_n(F)$，使得$\rho^*(x) = S^{-1}\rho(x)S$对于每个$x \in G$都成立. 我们注意到，如果$S$是$L_n(F)$的非奇异矩阵而且$\rho(x)$是$G$在$L_n(F)$中的表示，则$S^{-1}\rho(x)S = \rho^*(x)$也是$G$的表示. 事实上，如果我们把$\rho(x)$，$x \in G$看做$F$上具有基底$u_1, u_2, \cdots, u_n$的向量空间$V$到自身的线性变换的群而且

$$\begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{bmatrix} = S \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix},$$

---

1) 矩阵、行列式和完全线性群的性质可以参看 Birkhoff and MacLane [1] 第六到第十章.

2) Tr $\rho(x)$ 是指矩阵 $\rho(x)$ 的迹，即 $\rho(x)$ 的主对角元素的和. ——译者

则 $S^{-1}\rho(x)S=\rho^*(x)$，$x\in G$ 是V的同一些线性变换以基底 $v_1, v_2, \cdots, v_n$ 表出的群:

引理 16.2.1. 特征标是共轭类的函数，即共轭元素有相同的特征标.

引理 16.2.2. 等价的表示有相同的特征标.

事实上,如果A是n阶矩阵,则它的特征多项式是 $f(\lambda)=|A-\lambda I|=(-1)^n[\lambda^n-a_1\lambda^{n-1}+\cdots+(-1)^n a_n]$. 这里系数 a_1 是A的迹: $a_1=\operatorname{Tr}(A)$，而且 $a_n=|A|$ 是A的行列式. 现在如果T是非奇异矩阵,则

$$|T^{-1}AT-\lambda I|=|T^{-1}(A-\lambda I)T|$$
$$=|T^{-1}|\cdot|A-\lambda I|\cdot|T|=|A-\lambda I|.$$

因而A和 $T^{-1}AT$ 有相同的特征多项式，当然更有相同的迹. 因此 $\rho(y^{-1}xy)=\rho(y)^{-1}\rho(x)\rho(y)$ 和 $\rho(x)$ 有相同的迹，所以 $\chi(y^{-1}xy)=\chi(x)$,即特征标是共轭类的函数. 同理,$\rho^*(x)=S^{-1}\rho(x)S$ 和 $\rho(x)$有相同的迹，因而等价的表示有相同的特征标.

我们知道，域F上的向量空间(或线性空间)V由下列定律给定:

V具有二元加法：对于 $\alpha,\beta\in V$ 有 $\alpha+\beta\in V$.

V具有系数乘法 $c\alpha$ 对于 $c\in F$ 和 $\alpha\in V$.

这两种运算满足

$V1$) V 在加法下是阿贝尔群.

$V2$) $c(\alpha+\beta)=c\alpha+c\beta$, $(c+c')\alpha=c\alpha+c'\alpha$.

$V3$) $(cc')\alpha=c(c'\alpha)$; $1\alpha=\alpha$.

这里 $\alpha,\beta\in V$, $c, c'\in F$, 1 是F的单位元素.

V的向量 $u_1,\cdots,u_r$ 叫做线性无关的,如果从

$$a_1u_1+\cdots+a_ru_r=0,\ a_i\in F$$

得出 $a_1=\cdots=a_r=0$. 其次, $u_1,\cdots,u_n$ 叫做V的基底,如

果它们是线性无关的，而且每个 $u \in V$ 可以表成

$$u = b_1u_1 + \cdots + b_nu_n, b_i \in F.$$

如果 V 具有基底，则每一个基底包含同样个数的元素，这个数叫做向量空间的维数.

我们定义 $F-G$ 模 M 为 F 上的向量空间 V，它以 G 的元素作为 V 的算子，满足

1) $(u+v)g = ug + vg$, $u, v \in V$, $g \in G$.

2) $u(g_1g_2) = (ug_1)g_2$, $u \in V$, $g_1, g_2 \in G$.

3) $u \cdot 1 = u$, $u \in V$, 1 是 G 的单位元素.

4) $(au)g = a(ug)$, $a \in F$, $u \in V$, $g \in G$.

我们把 M 叫做 G 的表示模.

从 $F-G$ 模 M_1 到另一个 $F-G$ 模 M_2 的算子同态是指映射 $M_1 \to M_2$，使得

1) 如果 $u_1 \to v_1$, $u_2 \to v_2$, 则 $u_1 + u_2 \to v_1 + v_2$.

2) 如果 $u \to v$, $b \in F$, 则 $bu \to bv$.

3) 如果 $u \to v$, $g \in G$, 则 $ug \to vg$.

M_1 和 M_2 的算子同构是指从 M_1 到 M_2 的一一的算子同态.

现在设 M 是 $F-G$ 模而且具有基底 $u_1, \cdots, u_n$. 如果对于 $x \in G$，我们取映射 $v \to vx$, $v \in V$，使得

$$u_i \to u_ix = \sum_{j=1}^{n} a_{ij}u_j,$$

$i = 1, \cdots, n$, 则 $\rho(x) = (a_{ij})$, $i, j = 1, \cdots, n$ 就是 G 到 M 的表示，反之，设 ρ 是 G 在具有基底 $u_1, \cdots, u_n$ 的向量空间 V 上的表示，而且 $\rho(x) = (a_{ij}) = [a_{ij}(x)]$. 对于每个 $x \in G$，令

$$u_ix = \sum_{j=1}^{n} a_{ij}(x)u_j, \quad i = 1, \cdots, n.$$

那么，因为 $\rho(1) = I_n$ 而且 $\rho(xy) = \rho(x)\rho(y)$，所以 V 就成为 $F-G$ 模 M. 因此每个 n 维的 $F-G$ 模决定 G 的一个 n 阶

表示,反之亦然.

定理 16.2.1. 两个 $F-G$ 模 M_1 和 M_2 给出 G 的等价的表示，必要而且只要它们是算子同构的.

证明. 设给了 G 的两个等价的表示:

$$\rho(x) \text{ 和 } S^{-1}\rho(x)S, \ x \in G.$$

那么当 $\rho(x) = [a_{ij}(x)]$, $x \in G$ 时,这对应于以 G 作为算子群的向量空间 V 的基底 $u_1, \cdots, u_n$ 和映射 $u_i \to u_i x = \Sigma a_{ij}(x) u_j$. 我们已经说过 V 的这个映射

$$w \to wx, \ w \in V$$

还以基底 $v_1, \cdots, v_n$ 而对应于表示 $\rho^*(x) = S^{-1}\rho(x)S$, $x \in G$, 这里

$$\begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{bmatrix} = S \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix}.$$

如果 $S = (s_{ij})$, 则等价的表示 $\rho(x)$ 和 $\rho^*(x)$ 对于由

$$u_i \to \sum_j s_{ij} v_j, \ i = 1, \cdots, n$$

决定的映射而说是算子同构的. 反之, 设两个 $F-G$ 模 M_1 和 M_2 是算子同构的. 作为同构的向量空间, M_1 和 M_2 必定有同样个数的基元素. 设 M_1 的基底是 $u_1, \cdots, u_n$, 因而在算子同构下, $u_1, \cdots, u_n$ 映成 M_2 的基底 $v_1, \cdots, v_n$. 随同 $u_i \to v_i$ 取 $u_i x \to v_i x$, 于是对于这两个基底说来, M_1 和 M_2 产生相同的表示,因为如果

$$u_i x = \sum_{j=1}^{n} a_{ij}(x) u_j, \ i = 1, \cdots, n,$$

则必定有

$$v_i x = \sum_{j=1}^{n} a_{ij}(x) v_j,\ i = 1, \cdots, n.$$

因此等价的表示 $\rho(x)$ 和 $\rho^*(x)$ 对应于表示模的算子同构.

16.3. 完全可约性定理

假设表示模M具有子模 M_1, 它也是表示模. 我们取 M_1 的基底 $u_1, \cdots, u_r$ 而且取元素 $u_{r+1}, \cdots, u_n$ 来补成 M 的基底. 对应的表示 ρ 叫做可约的,对于基底 $u_1, \cdots, u_n$ 它具有形状

$$\rho(x) = \left(\begin{array}{c|c} \sigma(x) & 0 \\ \hline \theta(x) & \tau(x) \end{array}\right),$$

这里 σ 和 τ 分别是G的 r 阶和 $n-r$ 阶表示. 表示 σ 对应于具有基底 $u_1, \cdots, u_r$ 的 F-G 模 M_1. 至于 τ, 它是由具有基底 $M_1 + u_{r+1}, \cdots, M_1 + u_n$ 的商模 M/M_1 决定的表示. 更一般地, 如果

$$0 = M_0 \subset M_1 \subset M_2 \subset \cdots \subset M_k = M$$

是子模的链而且取M的对应于这个链的基底, 则对应的表示 ρ 取形状

$$\rho(x) = \begin{pmatrix} \rho_1(x) & & & 0 \\ & \rho_2(x) & & \\ & & \ddots & \\ * & & & \rho_k(x) \end{pmatrix},$$

这里 $\rho_i(x)$ 是对应于 M_i/M_{i-1} 的适当基底的表示, 这基底是 $M_{i-1} + u_j$, 这里 u_j 遍历属于 M_i 而不属于 M_{i-1} 的基元素. 对于特征标,我们显然有

$$\chi(x) = \chi_1(x) + \chi_2(x) + \cdots + \chi_k(x).$$

如果上面的链是极大的, 即它不能再加细, 则 M_i/M_{i-1} 没有

表示真子模，因而它们给出的是不可约表示 ρ_i. 由此得出以下的显然结果:

引理 16.3.1. 每个特征标是不可约特征标的和.

引理 16.3.2. 不可约表示 ρ_i 在不考虑先后顺序和算子同构的意义下是唯一决定的.

引理 16.3.2 从约当-霍德尔定理得出.

如果表示模 M 具有子模 M_1 也是表示模，则可以存在补充的表示子模 M_2，使得 M 是它们的直和: $M = M_1 \oplus M_2$. 在这种情形下，M_2 显然算子同构于 M/M_2，而且表示 $\rho(x)$ 有形状

$$\rho(x) = \left(\begin{array}{c|c} \rho_1(x) & 0 \\ \hline 0 & \rho_2(x) \end{array}\right).$$

反之，如果表示 $\rho(x)$ 具有这种对角分块的形状，则 M 是表示子模 M_1 和 M_2 的直和. 在这种情形下我们说已知表示是完全可约的. 并非每个可约的表示都是完全可约的. 例如由元素 b 生成的无限循环群的表示

$$\rho(b^i) = \begin{pmatrix} 1, & 0 \\ i, & 1 \end{pmatrix}$$

是可约的，而如果它是完全可约的，则它将把每个元素表示成单位元素，因为这时 $\rho_1(b^i)$ 和 $\rho_2(b^i)$ 都是单位元素. 然而

$$\begin{pmatrix} 1, & 0 \\ 1, & 1 \end{pmatrix}$$

并不与单位元素共轭，因而这显然是不可能的. 不过我们有重要的一类表示，对于它们说，可约的表示是完全可约的.

定理 16.3.1. 完全可约性定理. 如果域 F 的特征不整除有限群 G 的阶，则群 G 在域 F 上的可约的表示是完全可约的.

证明. 设 M 是 G 在 F 上的表示模而且 M_1 是表示子模. 取 M_1 的基底 $u_1, \cdots, u_r$，用元素 $u_{r+1}, \cdots, u_n$ 把它补成

M的基底. $u_{r+1},\cdots,u_n$ 是一个子空间N的基底,但是N一般不是表示模. 对于 $x\in G$ 有

$$\rho(x)=\left(\begin{array}{c|c}\sigma(x) & 0\\ \theta(x) & \tau(x)\end{array}\right).$$

我们还有 $M=M_1+N$, 而且对于 $u\in M$, 唯一地有

$$u=u_1+v,\ u_1\in M_1,\ v\in N.$$

映射 $\eta:u\to v$ 是幂等的和线性的,设 g 是G的阶,令

$$u'=\frac{1}{g}\sum_{x\in G}ux\eta x^{-1}=u\zeta.$$

这时 $u\to u'=u\zeta$ 是线性映射. 这个映射要求被G的阶 g 除的可能性,而由于根据假设,G的有限阶 g 不被 F 的特征整除,这确实是可能的.

设 $y\in G$, 令 $z=y^{-1}x$ 对于 $x\in G$, 于是

$$(u\zeta)y=\frac{1}{g}\sum_x ux\eta x^{-1}y=\frac{1}{g}\sum_z (uy)z\eta z^{-1}=(uy)\zeta,$$

因为 z 随 x 遍历 G. 这说明 $M_2=M\zeta$ 是表示模. 需要证明 $M=M_1\oplus M_2$, 为此必须证明每个 $u\in M$ 都能写成 $u=u_1+u_2,u_1\in M_1,\ u_2\in M_2$,而且这个式子是唯一的,即从 $0=u_1+u_2$ 得出 $u_1=0=u_2$. 对于任何 $u\in M$, 记

$$u=(u-u\zeta)+u\zeta.$$

这里 $u\zeta=u_2\in M_2$. 现在

$$u-u\zeta=\frac{1}{g}\sum_x (ux-ux\eta)x^{-1},$$

因为 $uxx^{-1}=u$. 但是 $ux-ux\eta=(ux)_1\in M_1$, 因而 $u-u\zeta=u_1\in M_1$. 因此 $u=u_1+u_2$, 这里 $u_1\in M_1,\ u_2\in M_2$. 现在如果 $w\in M_1$, 则 $wx\in M_1,\ wx\eta=0$, 因而 $w\zeta=0$. 因此对于任意 $u\in M$ 有 $(u-u\zeta)\zeta=0$, 即 $u\zeta^2=u\zeta$. 因此,如果 $u_1+u_2=0$, 则 $u_1\zeta+u_2\zeta=0$, 于是 $0+u_2\zeta=u_2=0$, 同

时还有 $u_1=0$. 所以已知表示是完全可约的.

利用矩阵的第二个证明: 设

$$\rho(x)=\left(\begin{array}{c|c}\sigma(x) & 0\\ \theta(x) & \tau(x)\end{array}\right),$$

这里 $\sigma(x)$ 和 $\tau(x)$ 分别是 r 阶和 $n-r$ 阶的表示. 我们希望找出矩阵

$$S=\left(\begin{array}{c|c}I_r & 0\\ \mu & I_{n-r}\end{array}\right),$$

这里 μ 不依赖于 x, 使得对于所有 $x\in G$ 都有

$$\left(\begin{array}{c|c}\sigma(x) & 0\\ \theta(x) & \tau(x)\end{array}\right)\left(\begin{array}{c|c}I_r & 0\\ \mu & I_{n-r}\end{array}\right)=\left(\begin{array}{c|c}I_r & 0\\ \mu & I_{n-r}\end{array}\right)\left(\begin{array}{c|c}\sigma(x) & 0\\ 0 & \tau(x)\end{array}\right).$$

明显地, 如果 S 能找到, 则它是非奇异的而且导出对于所有 $x\in G$ 的等价的表示

$$\rho^*(x)=S^{-1}\rho(x)S=\left(\begin{array}{c|c}\sigma(x) & 0\\ 0 & \tau(x)\end{array}\right),$$

$\rho^*(x)$是完全可约的. 这需要找出不依赖于 x 的 $(n-r)\times r$ 矩阵 μ, 使得对于所有 $x\in G$, 都有

$$\mu\sigma(x)-\tau(x)\mu=\theta(x).$$

根据 $\rho(yx)=\rho(y)\rho(x)$, 我们有

$$\theta(yx)=\theta(y)\sigma(x)+\tau(y)\theta(x),$$

因而

$$\theta(x)=\tau(y^{-1})\theta(yx)-\tau(y^{-1})\theta(y)\sigma(x),$$

而且

$$\theta(x)=\frac{1}{g}\sum_y(\tau(x)\tau(x^{-1}y^{-1})\theta(yx)-\tau(y^{-1})\theta(y)\sigma(x)).$$

因此,如果令

$$-\mu=\frac{1}{g}\sum_y\tau(y^{-1})\theta(y)=\frac{1}{g}\sum_y\tau(x^{-1}y^{-1})\theta(yx),$$

则就有 $\theta(x)=-\tau(x)\mu+\mu\sigma(x)$. 总之我们找到了适当的

$(n-r)\times r$ 矩阵 μ，所以变换矩阵 S 存在，而且等价的表示 $\rho^*(x)$是完全可约的.

重复应用这个定理,可以得出下列主要结果:

定理 16.3.2. 如果域 F 的特征不整除有限群 G 的阶，则群 G 在域 F 上的每一个表示可以完全地简化成不可约表示的和.

推论 16.3.1. 当域 F 的特征不整除有限群 G 的阶时，群 G 在域 F 上的表示等价，必要而且只要它们简化成同一些不可约表示的和，而且同一个不可约表示具有相同的重数.

当表示 ρ 完全可约时,我们记

$$\rho=\rho_1\oplus\rho_2\oplus\cdots\oplus\rho_k.$$

这里不可约表示 ρ_i 的顺序是不重要的，因为改变表示模的对应基底就能改变 ρ_i 的顺序. 当然，这些 ρ_i 是 M 看作以 F 和 G 为算子的加法群时的合成因子. 根据约当-霍尔德定理,不考虑顺序和算子同构，这些合成因子是唯一的. 根据定理16.1.1，不可约表示的算子同构表明等价性. 因而在推论里所说的“同一些不可约表示”并不区别等价的表示.

16.4. 半单纯的群环[1]和普通表示

给了任何群 G 和域 F,我们可以用下列方式构造群环 R_G:

1） R_G 是 F 上以元素 $g_i\in G$ 作为基底的向量空间.

2） 乘法定义为:

$$\sum_i a_i g_i \sum_j b_j g_j = \sum_{i,j} a_i b_j g_{ij},$$

这里 $g_{ij}=g_ig_j$ 属于 G.

1） 作者所说的环常常也指域上的代数. ——俄译者注

不难证明这个定义使 R_G 成为结合环而且具有单位元素 $1\cdot 1=1$，这是F的单位元素和G的单位元素的乘积. 明显地，如果用G的元素右乘而作用于 R_G 的元素，则 R_G 可以看作G的表示模. 如果G具有有限的阶 n，则取G的元素 $g_1,\cdots,g_n$ 作为 R_G 的基底时，对应的表示是

$$\rho(x)=(x_{ij}),\quad i,j=1,\cdots,n,\ x\in G,$$

这里当 $g_ix=g_j$ 时，$x_{ij}=1$，否则 $x_{ij}=0$. 这就是我们提到过的G的右正则表示，它作为置换群由下列式子给定

$$\pi(x)=\begin{pmatrix} g_1, & \cdots, & g_n \\ g_1x, & \cdots, & g_nx \end{pmatrix},\ x\in G,$$

现在写出的是矩阵形式.

引理 16.4.1. 在 n 阶群G的右正则表示 $\rho(x)$ 中，我们有 $\chi(1)=n$; $\chi(g)=0$, $g\neq 1$.

事实上，这时 $\rho(x)=(x_{ij})$，这里当 $g_ix=g_j$ 时，$x_{ij}=1$，否则 $x_{ij}=0$，因而

$$\chi(x)=\sum_i x_{ii}.$$

如果 $x=1$，则 $g_i1=g_j=g_i$，因而 $x_{ii}=1$, $i=1,\cdots,n$，所以 $\chi(1)=n$. 而如果 $x=g\neq 1$，则 $x_{ii}=0$，因为除非 $x=1$, $g_ix=g_i$ 对于任何 g_i 都不可能成立.

我们将得出的结果几乎都是关于有限群G在域F上的表示的，而且群G的阶不被域F的特征整除. 我们把这种表示叫做普通表示. 当域上的特征能整除有限群G的阶时，群G在域F上的表示叫做模表示. 模表示的性质与普通表示的性质不同. 当然可以设想无限群的表示与有限群的表示在很多方面都有不同.

我们说环R是正则的，假如对于每个 $u\in R$，存在元素 $x\in R$，使得 $uxu=u$. 域F上的有限维的正则环叫做半单纯

的．有条件 $e^2=e$ 的元素 $e\neq 0$ 叫做幂等的．

定理 16.4.1. 有限群 G 在域 F 上的群环 R_G 是半单纯的，必要而且只要 F 的特征不整除 G 的阶．

证明. 设 G 是有限阶 g 的群．设 F 的特征整除 g，而且 $x_1,\cdots,x_g$ 是 G 的元素，我们在 R_G 内考虑元素 $u=x_1+\cdots+x_g$．这时 $x_iu=ux_i=u$．因此当 $x=a_1x_1+\cdots+a_gx_g$ 时，我们有 $ux=(a_1+\cdots+a_g)u$，因而

$$uxu=(a_1+\cdots+a_g)gu=0\neq u.$$

因此 R_G 不是半单纯的．

现在设 G 的阶 g 不被 F 的特征整除．我们来证明 R_G 是半单纯的，甚至还将证明 R_G 的更进一步的性质．设 $\mathfrak{a}_1$ 是 R_G 的任何右理想．那么 $\mathfrak{a}_1$ 是 R_G 的表示子模，而且反之，R_G 的表示子模是右理想．根据完全可约性定理，

$$R_G=\mathfrak{a}_1\oplus\mathfrak{a}_2,$$

这里 $\mathfrak{a}_2$ 是另一个右理想．于是 $1=a_1+a_2$，$a_1\in\mathfrak{a}_1$，$a_2\in\mathfrak{a}_2$，而且这个表达式是唯一的．然而这时 $a_1=a_1^2+a_2a_1$ 也成立，拿这与唯一的表达式 $a_1=a_1+0$ 比较，我们得出 $a_1^2=a_1$，$a_2a_1=0$．因而 $a_1=e$ 是幂等的，而且 $a_2=1-e$ 也是幂等的．于是对于 $x\in R_G$，我们有 $x=ex+(1-e)x$，这里 $ex\in\mathfrak{a}_1$．反之，如果 $y\in\mathfrak{a}_1$，则根据表达式的唯一性，我们有 $y=ey+(1-e)y=y+0$．因此 $\mathfrak{a}_1$ 是幂等元素 e 的主右理想 eR_G，所以 R_G 的每个右理想是一个幂等元素的主右理想．特别地，对于每个元素 u，存在幂等元素 e，使得 $uR_G=eR_G$．因此对于某个 x 有 $ux=e$，而且对于某个 y 有 $ey=u$，$eu=e^2y=ey=u$．因而 $u=eu=uxu$，所以 R_G 是正则的．

定理 16.4.2. 域 F 上的有限维的正则环 R 具有单位元素，而且它的每个右（或左）理想是一个幂等元素的主理想．

每个双侧理想是属于中心的一个幂等元素的主理想.

证明. 设R是域F中的有限维的正则环. 对于任意元素$u\in R$, 根据正则性存在元素x, 使得$uxu=u$. 这时取$e=ux$, 我们有$e^2=uxux=ux=e$, 又取$f=xu$, 我们有$f^2=xuxu=xu=f$. 其次, $u=uxu=eu=uf$, 因而$uR=eR$和$Ru=Rf$. 因此主右(或左)理想是幂等元素的主右(或左)理想. 考虑左理想$\mathfrak{a}$. 如果$\mathfrak{a}\neq 0$, 则它包含某个幂等元素$e_1\neq 0$, 因而$Re_1\subseteq\mathfrak{a}$. 假定$\mathfrak{a}\neq Re_1$. 那么就存在某个$x\in\mathfrak{a}$. $x\in Re_1$.

$$x=xe_1+(x-xe_1),$$

这里$x_1=xe_1\in Re_1$, 而且

$$x_2=x-xe_1,$$

这里$x_2e_1=0$.

设f是使$Rx_2=Rf$的幂等元素. 那么$f=wx_2$, $fe_1=wx_2e_1=0$. 现在令$e_2=e_1+f-e_1f$. 这时$e_1e_2=e_1$, $fe_1=f$. 因而

$$e_2^2=(e_1+f-e_1f)e_2=e_1+f-e_1f=e_2,$$

所以e_2是属于$\mathfrak{a}$的幂等元素而且Re_2包含e_1和f, 因而它包含Re_1和元素$x\notin Re_1$. 因此Re_2的维数大于Re_1. 继续下去,我们可以在$\mathfrak{a}$内进一步构造幂等元素e_3, e_4, $\cdots$, 使得每个Re_i都有较大的维数, 直到最后达到一个幂等元素e, 使得$\mathfrak{a}=Re$. 这证明每个左理想是一个幂等元素的主左理想. 同理可以证明每个右理想是一个幂等元素的主右理想. 如果$x\in eR$, 则对于某个w, $x=ew$而且$ex=e^2w=ew=x$, 因而e是eR的元素的左单位元素. 同理,对于$x\in Rf$, 我们有$xf=x$. 现在把整个环R同时看作左理想和右理想, 因而存在幂等元素e和f, 使得$R=eR=Rf$. 因此$ef=f=e$而且$ex=xe=x$, 所以$e=1$是R的单位元素.

R 的中心内的一个幂等元素 e 的倍数当然组成双侧理想. 我们希望反过来证明任意双侧理想是中心内的一个幂等元素的主理想. 现在对于适当的幂等元素 e 和 f, $\mathfrak{a} = eR = Rf$. 因此 $ef = f = e$, 所以 $\mathfrak{a} = eR = Re$. 又对于任意 $x \in R$, 我们有 $ex \in \mathfrak{a}$, 因而 $ex = exe$. 又 $xe \in \mathfrak{a}$, 因而 $xe = exe$. 因此$ex = xe$,所以 e 在 R 的中心内.

如果环 R 是半单纯的而且不包含 0 和 R 以外的双侧理想, 则 R 叫做**单纯的**. 我们用$\oplus$表示右理想的直和; 又用$\boxplus$表示双侧理想的直和.

定理 16.4.3. **半单纯环 R 是单纯环的直和** $R = R_1 \boxplus R_2 \boxplus \cdots \boxplus R_s$. **如果不考虑顺序, 则这些单纯环 R_i 是唯一确定的.**

证明. 设 R_1 是包含在 R 内的极小双侧理想. 那么 R_1 是 R 的中心内的幂等元素 e_1 的主理想. 于是对于 $x \in R$, $x = xe_1 + x(1-e_1)$. 因此 $R = R_1 \boxplus \bar{R}_1$, 这里 $\bar{R}_1$ 由全体形如 $x(1-e_1)$ 的元素组成. 现在 e_1 是 R_1 的单位元素, 因而 $\bar{e}_1 = 1 - e_1$ 是 $\bar{R}_1$ 的单位元素,而且对于 $x, y \in R_1$ 和 $z, w \in \bar{R}_1$, 我们有 $(x+z)+(y+w) = (x+y)+(z+w)$ 和 $(x+z)\cdot(y+w) = xy + zw$, 因为 $zy = ze_1(1-e_1)y = 0$, 同理 $xw = 0$. 因此在直和 $R_1 \boxplus \bar{R}_1$ 中,加法和乘法都可以把分量分开来计算,因此特别地,从 R 的正则性得出 R_1 和 $\bar{R}_1$ 各自的正则性. 继续取 $\bar{R}_1$ 的极小双侧理想 R_2, 而且找出关系 $\bar{R}_1 = R_2 \boxplus \bar{R}_2$. 以这个方法继续下去,最终得出

$$R = R_1 \boxplus R_2 \boxplus \cdots \boxplus R_s,$$

这里 $1 = e_1 + e_2 + \cdots + e_s$, $e_i (i = 1, \cdots, s)$ 都是 R 的中心内的幂等元素,而且 $e_ie_j = 0$, $i \neq j$.

对于

$$x = x_1 + x_2 + \cdots + x_s,$$

$$y = y_1 + y_2 + \cdots + y_s,$$

这里 x_i, $y_i \in R_i$, 我们有

$$x + y = (x_1 + y_1) + (x_2 + y_2) + \cdots + (x_s + y_s),$$

$$xy = x_1y_1 + x_2y_2 + \cdots + x_sy_s.$$

所以反过来,同一个域 F 上的单纯环 R 的直和是正则的,因而是半单纯的. 现在设 $\mathfrak{a}$ 是 R 的任意双侧理想,它是中心内的一个幂等元素 e 的主理想. 这时

$$e = e_1e + e_2e + \cdots + e_se.$$

因而对于某个 i 有 $e_ie \neq 0$. 但是如果 $\mathfrak{a}$ 是极小的而且 $e_ie = e_i$, 则 e_ie 的主理想是 R_i 的真子集, 又如果 $e_ie \neq e$, 则它是 $\mathfrak{a}$ 的真子集, 因此 $e_ie = e_i = e$, 所以 $\mathfrak{a} = R_i$. 这证明了直和的唯一性.

定理 16.4.4. 有限群 G 的任何普通的不可约表示等价于在 R_G 的某个极小右理想上的表示. R_G 的两个极小右理想给出等价的表示, 必要而且只要它们属于 R_G 的同一个单纯分支.

证明. G 的任何表示 ρ 产生 R_G 的一个表示,因为如果

$$h = \sum_{x \in G} a_x x, \ a_x \in F, \ x \in G$$

是 R_G 的任意元素,我们可以取 $\rho(h) = \Sigma a_x\rho(x)$, 这是 R_G 的表示. G 的等价的表示给出 R_G 的等价的表示,反之亦然.

G 的正则表示是 G 的以 R_G 作为 F-G 模的表示. 它的完全约简的形式是

$$R_G = e_1R_G \oplus e_2R_G \oplus \cdots \oplus e_tR_G,$$

这里 $1 = e_1 + e_2 + \cdots + e_t$, e_i 是幂等元素而且它们是正交的, 即 $e_i e_j = 0$ 对于 $i \neq j$. 这时每个 $e_i R_G$ 都是极小右理想. 现在设 $\rho(x)$ 是 G 的普通的不可约表示,因而也是 R_G 的这种表示. 设 M 是表示 ρ 的不可约 F-G 模. 那么 $M =$

$M\cdot 1=M(e_1+\cdots+e_t)$. 因此对于某个 e_i, $Me_i\neq 0$. 设 m 是M中的向量，使得 $me_i\neq 0$. 那么 $me_iR_G\neq 0$ 是G的表示模，它不是零而且包含在M内. 由于M是不可约的，我们必须有 $M=me_iR_G$. 对应

$$me_i\left(\sum_{x\in G}a_xx\right)\rightleftarrows e_i\sum_{x\in G}a_xx$$

是一一的，因为使 $me_ih=0$ 的元素 e_ih 组成右理想，它是 e_iR_G 的真子集，因而是零. 我们在表示模M和表示模 e_iR_G 之间有了算子同构，因而根据定理 16.1.1, $e(x)$ 等价于G在极小右理想 e_iR_G 上的表示.

在什么情况下两个极小右理想产生等价的表示? 极小右理想必定包含在唯一的极小双侧理想内. 设

$$R_G=R_1\boxplus R_2\boxplus\cdots\boxplus R_s$$

是分 R_G 成单纯理想（即极小双侧理想）之和的分解式. 这时 $1=e_1+e_2+\cdots+e_s$ 而且 e_i 是属于中心的幂等元素的正交组. 设 $e_{i1}R_G$ 和 $e_{i2}R_G$ 是属于同一个单纯理想 R_i 的两个极小右理想. 那么全体有限和 $u_1e_{i1}v_1+\cdots+u_me_{i1}v_m$ (u_k, $v_k\in R_G$) 组成双侧理想，于是因为 $e_i(e_{i1})e_i=e_{i1}\neq 0$ 属于这个集合，所以这集合是 R_i. 因此，对于适当的一些 u 和 v,

$$u_1e_{i1}v_1+\cdots+u_me_{i1}v_m=e_{i2}.$$

因为 $e_{i2}^2=e_{i2}$, 对于某个 j 有

$$e_{i2}u_je_{i1}v_j\neq 0.$$

于是 $e_{i1}v_jR_G\neq 0$, 而且因为这是包含在极小理想 $e_{i1}R_G$ 内的右理想，所以 $e_{i1}v_jR_G=e_{i1}R_G$. 因此对于 $h\in R_G$, 我们有在右理想 $e_{i1}R_G$ 和 $e_{i2}R_G$ 之间的算子同构 $we_{i1}h\rightleftarrows e_{i2}h$, 因而它们的表示是等价的. 这证明了属于同一个单纯理想的极小右理想给出相同的表示.

现在设 $e_{i1}R_G$ 和 $e_{j1}R_G$ 是分别属于单纯理想 R_i 和 R_j

$(i \neq j)$的极小右理想. 考虑$e_{i1}R_G$上的表示，对于e_i, e_j分别有映射：

$$e_i: e_{i1}h \to e_{i1}he_i = e_{i1}e_ih = e_{i1}h,$$

$$e_j: e_{i1}h \to e_{i1}he_j = e_{i1}e_jh = 0,$$

因而$\rho(e_i) = 1$和$\rho(e_j) = 0$. 同理,对于$e_{j1}R_G$上的表示，e_i映成0而且e_j映成1. 因此这两个表示不等价.

我们已经利用了分R_G成单纯理想的和来找出属于R_G的中心Z的正交幂等元素. 那么R_G的中心是什么呢？这是容易回答的.

定理 16.4.5. R_G的中心具有基底$C_i = x_{i1} + \cdots + x_{ih}$，这里$x_{i1}, \cdots, x_{ih}$组成群$G$的共轭类.

证明. 如果$C_i = x_{i1} + \cdots + x_{ih}$，这里$x_{i1}, \cdots, x_{ih}$组成$G$的共轭类，则对于$y \in G$, $y^{-1}C_iy = C_i$，因为用元素作变形只不过使共轭类中的元素彼此置换. 因为C_i与每个$y \in G$可交换，所以它与R_G的每个元素可交换,即它属于R_G的中心. 反之,如果u属于R_G的中心而且

$$u = \sum_{x \in G} a_x x,$$

则对于$y \in G$有

$$y^{-1}uy = u = \sum_{x \in G} a_x y^{-1}xy,$$

因而在u内共轭元素具有相同的系数,这说明u是C_i的线性组合

16.5. 绝对不可约表示. 单纯环的结构

我们已经知道不可约的普通表示作为群G的正则表示$R(G)$的分支而出现. 因而决定这种表示就成为找出$R(G)$的完全的简约,这也就是找出群环R_G的不可约的右理想.

表示的不可约性是依赖于基域的相对概念．例如当G是具有元素 $1, x, x^2$ 的 3 阶循环群时，在有理数域上的群环 R_G 有分解式 $R_G = R_1 \boxplus R_2$，这时 $1 = e_1 + e_2$，而且

$$e_1 = \frac{1 + x + x^2}{3},\ e_2 = \frac{2 - x - x^2}{3}$$

是幂等元素，R_1 以 e_1 作为基底，而 R_2 有基底 e_2, e_2x．这给出表示

$$\rho(x) = \left(\begin{array}{c|cc} 1 & 0, & 0 \\ \hline 0 & 0, & 1 \\ 0 & -1 & -1 \end{array}\right),$$

而且 R_1 和 R_2 给出 1 阶和 2 阶的不可约表示．但是如果我们增添 1 的立方根

$$\varepsilon = (-1 + \sqrt{-3})/2$$

来扩张有理数域，则 R_2 上的不可约表示就成为可约的了．取新的基底

$$e_1 = \frac{1 + x + x^2}{3},$$

$$\bar{e}_2 = \frac{1 + \varepsilon x + \varepsilon^2 x^2}{3},\ \bar{e}_3 = \frac{1 + \varepsilon^2 x + \varepsilon x^2}{3},$$

这时有 $\bar{e}_2 + \bar{e}_3 = e_2$；对于这新的基底有

$$\rho(x) = \begin{pmatrix} 1, & 0, & 0 \\ 0, & \varepsilon^2, & 0 \\ 0, & 0, & \varepsilon \end{pmatrix},\ \varepsilon^3 = 1.$$

明显地，域的进一步扩张不会再简约 $\rho(x)$ 了．

如果 n 阶表示 ρ 在扩张基域 F 时不能简约，则它叫做**绝对不可约的**．明显地，如果 ρ 在 $K \supset F$ 上可以简约，即

$$\rho(x) = \left(\begin{array}{c|c} \sigma(x) & 0 \\ \hline 0 & \tau(x) \end{array}\right)$$

对于所有 $x \in G$，这里 $\sigma(x)$ 是 $s \times s$ 矩阵，$\tau(x)$ 是 $(n - s) \times$

$(n-s)$ 矩阵，则 $\rho(h)$, $h\in R_G$ 作为K 上的代数，它的维数最多是 $s^2+(n-s)^2<n^2$. 因此，如果 $\rho(h)$, $h\in R_G$ 是F 上的 n^2 维的代数，则 ρ 是在 F 上绝对不可约的. 我们要来证明，在域的适当的代数扩张下，任何普通表示是不可约表示的直和，并且 n 阶的不可约表示是域上的 n^2 维的代数.

定理 16.5.1. 域 F 上的有限维的可除环[1] D 一般不是 F 的代数扩张上的可除环，唯一的例外是当 D 在 F 上的维数是一时，这时 $D=F$.

证明. 设 D 在 F 上的基底是 u_1, $\cdots$, u_n, 这里可以取 $u_1=1$ 为 D 的单位元素. 设 $n>1$, 考虑 $1=u_1, u_2, u_2^2, \cdots, u_2^n$. 它们在 F 上必定是线性相关的，即我们有等式

$$u_2^n+a_1u_2^{n-1}+\cdots+a_n=0,\quad a_i\in F.$$

因此，如果把 $f(x)=x^n+a_1x^{n-1}+\cdots+a_n$ 的根 $\alpha_1,\cdots,\alpha_r$ 增添到 F, 则就有 $(u_2-\alpha_1u_1)\cdots(u_2-\alpha_nu_1)=0$. 于是在 F 的这个代数扩张下，$u_2-\alpha_iu_1$ 都是零因子. 因此唯有在 $n=1$ 时 D 才是 F 的代数扩张上的可除环，而且这时 $D=F$.

定理 16.5.2. 单纯环 R 是包含 R 的可除环 D 上的完全矩阵环.

证明. 设 $e_{11}R$ 是 R 的极小右理想，e_{11} 是幂等元素. 那么 $1-e_{11}$ 是幂等元素而且 $R=e_{11}R\oplus(1-e_{11})R$. 如果 e_2R 是 $(1-e_{11})R$ 内的极小右理想，这里 e_2 是幂等元素，则我们有 $(1-e_{11})e_2=e_2$, 因而 $e_{11}e_2=0$. 又 $e_{22}=e_2-e_2e_{11}$ 是幂等元素，而且 $e_{22}R=e_2R$ 和 $e_{11}e_{22}=0$, $e_{22}e_{11}=0$. 于是 $R=e_{11}R\oplus e_{22}R\oplus(1-e_{11}-e_{22})R$. 现在假定已经找出正交的幂等元素 $e_{11},\cdots,e_{ii}$, 使得 $e_{ii}R$ 是极小右理想，而且

$$R=e_{11}R\oplus e_{22}R\oplus\cdots\oplus e_{ii}R\oplus(1-e_{11}-\cdots-e_{ii})R.$$

---

1) 也叫做体. ——译者

设 e_{i+1} 是幂等元素，使得 $e_{i+1}R$ 是 $(1-e_{11}-\cdots-e_{ii})R$ 内的极小右理想．那么 $e_{i+1}=(1-e_{11}-\cdots-e_{ii})e_{i+1}$，因而 $e_{jj}e_{i+1}=e_{jj}(1-e_{11}-\cdots-e_{ii})\ e_{i+1}=0,\ j=1,\ \cdots,\ i$．如果令 $e_{i+1,i+1}=e_{i+1}(1-e_{11}-\cdots-e_{ii})$，则 $e_{i+1,i+1}$ 是幂等元素，$e_{i+1,i+1}R=e_{i+1}R$，而且 $e_{i+1,i+1}$ 与 $e_{11},\ \cdots,\ e_{ii}$ 也正交．继续下去，最终得出

$$R=e_{11}R\oplus e_{22}R\oplus\cdots\oplus e_{nn}R,$$

这里 e_{ii} 是正交的幂等元素，$e_{ii}R$ 是极小右理想，而且

$$1=e_{11}+\cdots+e_{nn}.$$

引理 16.5.1. $e_{ii}Re_{jj}\neq 0$ 对于 $i,j=1,\cdots,n$．

证明．全体有限和 $\sum\limits_k u_ke_{ii}v_k$ 组成包含 $e_{ii}\neq 0$ 的双侧理想，因而这些和组成整个环 R．因此对于适当的元素 u_k，v_k，我们有 $\Sigma u_ke_{ii}v_k=e_{jj}$，于是 $\Sigma u_ke_{ii}v_ke_{jj}=e_{jj}$．因此对于某个 v，$e_{ii}ve_{jj}\neq 0$．

引理 16.5.2. $e_{ii}Re_{ii}$ 是可除环(记做 D_i)．

证明．$e_{ii}Re_{ii}$ 当然是在加法和乘法下闭合的，因而它是 R 的子环．它以 e_{ii} 作为单位元素．只需要找出不是 0 的元素的逆．如果 $e_{ii}xe_{ii}\neq 0$，则 $e_{ii}xe_{ii}R$ 是 $\neq 0$ 的右理想，它包含于（因而就等于）极小右理想 $e_{ii}R$．因此对于某个 y，$e_{ii}xe_{ii}y=e_{ii}$，所以 $e_{ii}xe_{ii}\cdot e_{ii}ye_{ii}=e_{ii}$．于是 $e_{ii}ye_{ii}$ 是 $e_{ii}xe_{ii}$ 在 $e_{ii}Re_{ii}$ 内的逆，所以 $e_{ii}Re_{ii}$ 是可除环．

对于每个 $i=2,\cdots,n$ 取一个元素 $e_{11}be_{ii}\neq 0$，而且记 $e_{11}be_{ii}=e_{1i}$．那么

$$e_{11}e_{1i}=e_{1i}e_{ii}=e_{1i}.$$

因为 $e_{1i}R\subseteq e_{11}R$，所以 $e_{1i}R=e_{11}R$．因此对于某个 y，$e_{1i}y=e_{11}$，$e_{1i}(e_{ii}ye_{11})=e_{11}$．记 $e_{i1}=e_{ii}ye_{11}$．那么对于 $i=2,\cdots,n$，

$$e_{ii}e_{i1}=e_{i1}e_{11}=e_{i1},\ e_{1i}e_{i1}=e_{11}.$$

因此 $e_{1i}e_{i1}e_{1i}e_{i1}=e_{11}^2=e_{11}$，所以 $e_{i1}e_{1i}\neq 0$。然而 $(e_{i1}e_{1i})^2=e_{i1}e_{1i}$，这说明它是 $e_{ii}Re_{ii}$ 内的幂等元素，因而 $e_{i1}e_{1i}=e_{ii}$，因为在除环内单位元素是唯一的非零幂等元素。现在在 $i\neq j$ 时令 $e_{i1}e_{1j}=e_{ij}$。那么我们有 $e_{ij}e_{jk}=e_{i1}e_{1j}e_{j1}e_{1k}=e_{i1}e_{11}e_{1k}=e_{i1}e_{1k}=e_{ik}$。又如果 $j\neq k$，则 $e_{ij}e_{kt}=e_{ij}e_{jj}e_{kk}e_{kt}=0$。因此对于这 n^2 个 e_{ij}，我们已经证明了下列结论：

$$e_{ij}e_{kt}=\delta_{jk}e_{it},\ \delta_{jj}=1,\ \delta_{jk}=0,\ j\neq k,$$

所以 e_{ij} 具有与下列 $n\times n$ 矩阵相同的乘法性质：

$$E_{ij}=(a_{rs}),\quad i,j=1,\cdots,n,$$

这里 $a_{ij}=1$，而当 $(r,s)\neq(i,j)$ 时，$a_{rs}=0$。

现在从可除环 $D_1=e_{11}Re_{11}$ 定义环 D，D 的元素 d 是：

$$d=d_1+e_{21}d_1e_{12}+\cdots+e_{n1}d_1e_{1n},$$

对于每个 $d_1\in D_1$。我们不难验证 D 同构于 D_1，因而它也是可除环．对应于 D_1 的单位元素，我们有 $e_{11}+e_{22}+\cdots+e_{nn}=1$，它是 D 的单位元素也是 R 的单位元素．又对于 $d\in D$，我们有 $e_{ij}d=e_{i1}d_1e_{1j}=de_{ij}$。

最后，对于任意 $x\in R$，我们有

$$x=1x1=(e_{11}+\cdots+e_{nn})x(e_{11}+\cdots+e_{nn})$$
$$=\sum_{i,j}e_{ii}xe_{jj}.$$

而这时

$$x_{ij}=e_{ii}xe_{jj}=e_{i1}e_{1i}xe_{j1}e_{1j}=e_{i1}u_1e_{1j}$$

对于某个 $u_1\in D_1$，因而对于 $u\in D$，我们有 $x_{ij}=ue_{ij}=e_{ij}u$。这就完成了定理的证明．我们证明了，单纯环 R 可以用可除环 D 上的 $n\times n$ 矩阵环以明白方式表出，这时 D 的单位元素与环 R 的单位元素相同．

定理 16.5.3. 如果R_G是域F上的半单纯群环，则就存在F的代数扩张F^*，使得R_G是F^*上的完全矩阵环的直和。我们可以取F^*为F的有限代数扩张.

证明. R_G在域F上是半单纯的，必要而且只要域F的特征不整除群G的阶. 这个性质并不因为把F换成F的代数扩张F^*而改变. 如果在把F上的R_G表成单纯环的直和的分解式$R_1 \boxplus \cdots \boxplus R_t$中，存在某个单纯环$R_k$，它所对应的可除环$D$不是域$F$，则在作$F$的某个代数扩张$F^*$时，环$D$不再是可除环. 这样就将以下列两种方式之一而改变$R_G$的分解式：(1) 增加（而决不会减少）了在$R_G$的中心内的幂等元素的个数，因而使一个单纯环解体成若干个单纯环的直和；(2) 在单纯环R_k内找到较低维的可除环D^*，而且R_k表成D^*上的较高维的矩阵环. 这两种情形都会出现. 我们已经看到过在3阶群的表示中出现第一种情形. 第二种情形出现在四元数群Q在有理数域F上的环R_Q中. F上的R_Q是四个1维单纯环和一个4维单纯环的直和，这个4维单纯环是可除环（四元数代数）. 如果我们把i增添到F，这个可除环变成复有理数上的2×2矩阵的环.

在任何情况下，F的代数闭包$\bar{F}$是这样的域，在这域上R_G中出现的每个单纯环R_k都是$\bar{F}$上的矩阵环. 单纯环R_k的矩阵单位元素e_{ij}^k可以用G的元素x表出，而且包含着出现在这些表达式中的全体系数的任何域F^*都有性质：R_k是F^*上的完全矩阵环. F^*显然是F的有限扩张.

定理 16.5.4. 域F上的完全矩阵环R_k的中心由R_k的单位元素（单位矩阵）的数量倍数组成. 域F上的矩阵环的直和$R = R_1 + \cdots + R_r$的中心以$R_1, \cdots, R_r$的r个单位元素作为它的基底.

证明. 设R_k是F上的完全$n \times n$矩阵环. 假定

$$x=\sum_{i,j}a_{ij}e_{ij},\quad a_{ij}\in F$$

属于 R_k 的中心. 从 $e_{rs}x=xe_{rs}$ 得出

$$\sum_j a_{sj}e_{rj}=\sum_i a_{ir}e_{is}.$$

因此当 $j\neq s$ 时 $a_{sj}=0$, 而且 $a_{ss}=a_{rr}$. 于是

$$x=a_{11}(e_{11}+\cdots+e_{nn})=a_{11}\cdot 1,$$

而且所有这种元素都属于 R_k 的中心. 如果

$$R=R_1+\cdots+R_r,$$

则 R 的中心是 R_k 的中心的直和，因而它以这些 R_k 的 r 个单位元素作为基底.

我们已经得到了联系 G 的普通表示和半单纯群环 R_G 的一系列定理. 我们把这些结果合成一个定理.

定理 16.5.5. 有限群 G 的每一个不可约的普通表示都是右正则表示 $R(G)$ 的一个分支. 不等价的绝对不可约表示的个数等于 G 的共轭类的个数. 如果 $\rho_1,\cdots,\rho_r$ 是不同的绝对不可约表示，而且 ρ_i 的阶是 n_i; $i=1,\cdots,r$, 则 ρ_i 在 F 上的维数是 n_i^2, 而且 ρ_i 在 $R(G)$ 内出现 n_i 次. 与 $\rho_i(x)$ (对于所有 $x\in G$) 可交换的矩阵只有单位矩阵的数量倍. 如果 g 是 G 的阶，则 $g=n_1^2+n_2^2+\cdots+n_r^2$.

证明. 根据定理 16.4.4, 每个普通的不可约表示等价于在 R_G 的某个极小右理想上的表示，因而是 $R(G)$ 的一个分支. 又不等价的不可约表示的个数等于 R_G 中的单纯理想的个数. 必要时把域 F 扩张成 F^*, R_G 的中心具有由 r 个幂等元素组成的基底，因而根据定理 16.5.4, R_G 是 r 个矩阵环的直和. 但是根据定理 16.4.5, R_G 的中心以各共轭类元素的和 C_i 作为基底, 因而 r 是 G 的共轭类的个数. 在 F^* 上, 在 R_i 中出现的极小右理想是 $e_{11}R$, 而且当 R_i 是 $n\times n$ 矩阵环时，它

具有基底 $e_{11}, e_{12}, \cdots, e_{1n_i}$. 对应的表示 ρ_i 的阶是 n_i，而且当 ρ_i 扩张成 R_G 的表示时将会一一地表示单纯环 R_i，但是把所有其他的 R_j 表示成 0，因为在定理 16.4.4 的证明里曾经指出过，如果 e_j 是 R_j 的单位元素 $(j \neq i)$，则 $\rho_i(e_j) = 0$. 因此 $\rho_i(R_G)$ 是 F^* 上的 n_i^2 维的完全矩阵环，于是它当然是绝对不可约的，因为进一步的简约只有当它在 F^* 上有较低的维数时才有可能. 又由于维数是 n_i^2，所以与每个 $\rho_i(x)$，$x \in G$ 可交换的矩阵只可能是单位矩阵的数量倍. 最后，因为每个 R_i 有由 n_i^2 个元素组成的基底，所以它们的直和的基底包含 $n_1^2 + \cdots + n_r^2$ 个元素. 但是 R_G 以 G 的 g 个元素作为基底. 因此

$$g = n_1^2 + \cdots + n_r^2.$$

R_i 是 n_i 个右理想 $e_{11}R, \cdots, e_{n_in_i}R$ 的直和，因而 ρ_i 在 $R(G)$ 内出现 n_i 次.

16.6. 在普通特征标之间的关系

上一节探讨了群 G 的这种表示，它取决于 R_G 的本质和 G 的表示给出 R_G 的表示的事实. 在本节中我们将寻求特征标 $\chi(x)(x \in G)$之间的关系. 它们与 G 本身的关系比与 R_G 的关系更为密切. 在本节中我们谈的都是普通表示.

定理 16.6.1. 设 A 和 B 是两个 F-G 模. 如果 A 有维数 m 而且产生表示 $\rho(x)$，$x \in G$，又 B 有维数 n 而且产生表示 $\sigma(x)$，则从 A 到 B 的算子同态的加法群同构于所有这种 $m \times n$ 矩阵 α 的加法群，它们使得 $\rho(x)\alpha = \alpha\sigma(x)$对于所有 $x \in G$.

推论 16.6.1. 从 A 到自身的算子自同态环同构于使 $\rho(x)\alpha = \alpha\rho(x)$的 $m \times m$ 矩阵 α 的环.

证明. 设 A 有基底 $u_1, \cdots, u_m$，B 有基底 $v_1, \cdots, v_n$. 那么从 A 到 B 的任何线性映射由基元素的像决定，设

$$u_1 \to a_{11}v_1 + \cdots + a_{1n}v_n,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$u_i \to a_{i1}v_1 + \cdots + a_{in}v_n,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$u_m \to a_{m1}v_1 + \cdots + a_{mn}v_n,$$

而且记 $\alpha = (a_{ij}), i = 1, \cdots, m; j = 1, \cdots, n$. 这些线性映射组成加法群，它同构于矩阵 α 的加法群. 如果这些线性映射还是算子同态，则当 $u \to v$ 时还有 $ux \to vx$ 对于 $x \in G$. 这说明映射 $u \to ux \xrightarrow{\alpha} vx$ 和 $u \xrightarrow{\alpha} v \to vx$ 重合，这就得出关系

$$\rho(x)\alpha = \alpha\sigma(x)$$

对于所有 $x \in G$.

当从 A 映到自身时，这映射就叫做**自同态**. 这时如果 α 和 β 是两个算子自同态，则我们有

$$\rho(x)(\alpha\beta) = [\rho(x)\alpha]\beta = [\alpha\rho(x)]\beta = (\alpha\beta)\rho(x),$$

因而使 $\rho(x)\alpha = \alpha\rho(x)$ 的矩阵 α 组成的环同构于 A 的算子自同态的环.

定理 16.6.2 对于任何 Ω 模都成立，这里 Ω 是指任何算子集合，当然我们主要关心的是 F-G 模的情形.

定理 16.6.2 (叔尔引理). *如果 A 和 B 是两个不可约的 Ω 模，则除它们是算子同构的情形外，从 A 到 B 的算子同态都把 A 映成 0. 如果 A 是不可约的，则 A 的不是恒等于零的算子自同态是算子同构.*

证明. 设 $u \in A$, $v \in B$, $\omega \in \Omega$. 那么如果对于某个 $u \in A$, 存在算子同态使 $u \to v \neq 0$, 则 $u\omega \to v\omega$ 对于所有 $\omega \in \Omega$. 这时 $u\Omega$ 是 A 的子模，因为 A 是不可约的，所以它是整个 A. 因此 $A = u\Omega \to v\Omega \neq 0$, 于是 $A \to v\Omega = B$. 这映射必定是一一的，因为否则 A 的映成零的非零元素组成 A 的 Ω 子模，这与 A 不可约的假设矛盾. 因此这映射是同构，因而特

别地，从 A 到自身的每个算子自同态是算子自同构.

定理 16.6.3. 如果 ρ 和 σ 是有限群 G 的不等价的不可约表示，它们的阶分别是 m 和 n，而且 ξ 是任意 $m\times n$ 矩阵，则

$$\sum_{y\in G}\rho(y)\xi\sigma(y^{-1})=0.$$

证明. 记

$$\alpha=\sum_{y\in G}\rho(y)\xi\sigma(y^{-1}).$$

那么对于 $x\in G$, $xy=z$, $y^{-1}=z^{-1}x$,

$$\rho(x)\alpha=\sum_{y}\rho(x)\rho(y)\xi\sigma(y^{-1})=\sum_{y}\rho(xy)\xi\sigma(y^{-1})$$

$$=\sum_{z}\rho(z)\xi\sigma(z^{-1})\sigma(x)=\alpha\sigma(x),$$

对于所有 $x\in G$.

因此，根据定理 16.6.1 和 16.6.2，当 ρ 和 σ 是不等价的不可约表示时，我们必定有 $\alpha=0$. 注意这些定理对于 G 在任何域上的表示都成立.

如果 $f_1(y)$ 和 $f_2(y)$ 是对于 $y\in G$ 定义而且在 F 内取值的两个函数（我们现在假定 F 的特征不整除 G 的阶），那么我们定义它们的对称的双线性纯量积为：

$$(f_1,f_2)=\frac{1}{g}\sum_{y\in G}f_1(y)f_2(y^{-1}).$$

由于 y^{-1} 随 y 而遍历 G，我们容易验证：

1) $(f_1,f_2)=(f_2,f_1)$.

2) $(f_1+f_2,f_3)=(f_1,f_3)+(f_2,f_3)$.

3) $(af_1,f_2)=a(f_1,f_2)$, $a\in F$.

现在假定 $\rho(x)$ 和 $\sigma(x)$ 是不等价的不可约表示. 如果在定理 16.6.3 里取 $\xi=e_{rs}$ 为在位置 (r,s) 处是 1 其他都是零的 $m\times n$ 矩阵，则就有

$$\alpha = (\alpha_{ij}),\ \alpha_{ij} = \sum_{y \in G} \rho_{ir}(y)\sigma_{sj}(y^{-1}),$$

这里

$$\rho(x) = (\rho_{ij}(x)),\ i, j = 1, \cdots, m;$$
$$\sigma(x) = (\sigma_{ij}(x)),\ i, j = 1, \cdots, n.$$

因为根据定理 16.6.1 和 16.6.2 有 $\alpha = 0$，所以 $(\rho_{ir}, \sigma_{sj}) = 0$. 我们还可以证明更多一些.

定理 16.6.4. 如果 ρ 和 σ 是有限群 G 的不等价的不可约的普通表示，则对于所有的 i, r, s, j，对称双线性纯量积 $(\rho_{ir}, \sigma_{sj}) = 0$. 如果 ρ 是 n 阶的绝对不可约的普通表示，则除 $i = j$, $r = s$ 外，$(\rho_{ir}, \sigma_{sj}) = 0$，因而对于所有 i, j，

$$(\rho_{ij}, \sigma_{ji}) = \frac{1}{n}.$$

证明. 我们已经证明了定理的第一部分. 现在来考虑 G 的绝对不可约的普通表示 ρ. 设 n 是 ρ 的阶，如果 ξ 是任意的 $n \times n$ 矩阵，则我们可以像前面一样地验证，

$$\alpha = \frac{1}{g} \sum_{y \in G} \rho(y)\xi\rho(y^{-1})$$

满足关系 $\rho(x)\alpha = \alpha\rho(x)$ 对于所有 $x \in G$. 因此根据定理 16.5.5，α 是单位矩阵的纯量倍 $\alpha = \lambda I_n$，这里系数 λ 取决于 ξ. 如果 $\xi = e_{rs}$，则记 $\lambda = \lambda_{rs}$. 于是 $\lambda_{rs}\delta_{ij} = (\rho_{ir}, \rho_{sj})$. 但是 $(\rho_{ir}, \rho_{sj}) = (\rho_{sj}, \rho_{ir})$，所以除 $i = j$ 并且 $r = s$ 外，$\lambda_{rs}\delta_{ij} = \lambda_{ji}\delta_{sr} = 0$，而且 $(\rho_{ij}, \rho_{ji}) = \lambda_{ii} = (\rho_{ji}, \rho_{ij}) = \lambda_{jj}$. 因此

$$\lambda_{11} = \lambda_{22} = \cdots = \lambda_{nn} = \lambda.$$

于是

$$n\lambda = \sum_{j} \lambda_{jj} = \frac{1}{g} \sum_{y, j} \rho_{ij}(y)\rho_{ji}(y^{-1})$$
$$= \frac{1}{g} \sum_{y} \rho_{ii}(1) = 1.$$

因此 $\lambda = 1/n$. 这证明了定理的其余部分. 注意 $n\lambda = 1$ 说明阶 n 不被 F 的特征整除.

可以把这些结果带到特征标上.

定理 16.6.5. 如果 χ, ϕ 是不同的不可约的特征标. 则 $(\chi, \phi) = 0$. 如果 χ 是绝对不可约的特征标,则 $(\chi, \chi) = 1$.

证明. 如果 χ 和 ϕ 是表示 ρ 和 σ 的不可约的特征标,则对于 $y \in G$,

$$\chi(y) = \sum_i \rho_{ii}(y), \quad \phi(y) = \sum_j \sigma_{jj}(y).$$

因为纯量积是双线性的,所以

$$(\chi, \phi) = \sum_{i,j} (\rho_{ii}, \sigma_{jj}) = 0,$$

因为和式中的每一项都是零. 现在设 χ 是 n 阶表示 ρ 的绝对不可约的特征标. 于是

$$(\chi,\chi) = \sum_{i,j} (\rho_{ii},\rho_{jj}) = \sum_{i,i} (\rho_{ii}, \rho_{ii}) = \sum_i \frac{1}{n} = 1.$$

这就完成了定理的证明.

推论 16.6.2. 对于恒同表示有 $\sum_{x \in G} \chi(x) = g$. 对于其他的不可约表示有 $\sum_{x \in G} \chi(x) = 0$.

事实上, 在恒同表示下对于任何 x 都有 $\chi(x) = 1$, 因而 $\sum_{x \in G} \chi(x) = g$. 而如果 χ 是任何其他不可约表示的特征标,取 ϕ 为恒同特征标,则 $(\chi,\phi) = 0$ 给出 $\frac{1}{g} \Sigma\chi(x) = 0$.

定理 16.6.6. 如果 χ, ϕ 是特征标而且 $\chi = \Sigma a_i\chi_i$, $\phi = \Sigma b_i\chi_i$, 这里 $\chi_i(i = 1, \cdots, r)$ 是绝对不可约特征标, 则 $(\chi, \phi) = \Sigma a_i b_i$. 因此,当域 F 的特征是零时, 对于特征标 ϕ, $(\phi, \phi) = 1$ 是 ϕ 作为绝对不可约特征标的必要而且充分的条件.

证明. 这个定理可以从定理 16.6.5 利用纯量积的双线性得出. 如果 $\phi = \Sigma c_i \chi_i$, 则 c_i 是非负的整数, 而且如果 $(\phi, \phi) = \Sigma c_i^2 = 1$, 则当域 F 的特征是零时, 可以得出 c_i 中有一个是 1 而且其余的是零.

定理 16.6.7. 阿贝尔群 G 的绝对不可约表示的阶都是1.

证明. 因为 G 是阿贝尔群, 所以它的所有元素属于同一个共轭类, 因而如果 g 是它的阶, 则我们有阶为 $n_1, \cdots, n_g$ 的 g 个绝对不可约表示, 这里 $g = n_1^2 + n_2^2 + \cdots + n_g^2$. 因此 $n_1 = n_2 = \cdots = n_g = 1$. 然而对于 1 阶的每个表示 $\rho(x)$, 我们有 $\chi(x) = \rho(x)$. 因此绝对不可约表示与特征标重合, 即它们就是在第十三章里讨论过的阿贝尔群的特征标.

定理 16.6.8. 设 x 是群 G 中的 m 阶元素, 又 ρ 是 G 的 n 阶表示. 那么, 必要时把 m 次单位根添加到 F, $\rho(x)$ 相似于以 m 次单位根作为对角元素的对角矩阵. 如果 F 是复数域, 则 $\chi(x^{-1}) = \overline{\chi(x)}$, 后者是 $\chi(x)$ 的共轭复数.

证明. 矩阵 $1, \rho(x), \cdots, \rho(x^{m-1})$ 是 m 阶循环群 C 的表示. 但是 C 的绝对不可约表示是 1 阶的; $\sigma(x) = (b)$, 这里因为 $1 = x^m$, 所以 $b^m = 1$, 因而 b 是 m 次单位根. 在 R_C 内容易验证, 当 ω 遍历全体 m 次单位根时,

$$\frac{1}{m}(1 + \omega x + \omega^2 x^2 + \cdots + \omega^{m-1} x^{m-1})$$

是产生不可约表示的幂等元素. 因此, 在把 m 次单位根添加到 F (它的特征当然不是 m 的约数) 后, C 的表示 $\rho(x)$ 完全简约, 而且我们得到相似于 $\rho(x)$ 的对角矩阵, 它的对角元素是 $b_1, \cdots, b_m$, 这里 b_i 都是 m 次单位根. 因此 $\chi(x) = b_1 + \cdots + b_n$. 于是 $\rho(x^{-1})$ 相似于以 $b_1^{-1}, \cdots, b_n^{-1}$ 为对角元素的对角矩阵, 而且 $\chi(x^{-1}) = b_1^{-1} + \cdots + b_n^{-1}$. 又如果 F 是复数域, 则任何次单位根的逆是它的共轭复数, 即 $b_i^{-1} = \bar{b}_i$, 所以

$\chi(x^{-1}) = \overline{\chi(x)}$.

设 ρ 是群 G 的任何表示，而且对于每个 $x \in G$，定义 $\hat{\rho}(x) = \rho(x^{-1})^T$，这里用 T 表示矩阵的转置. 那么

$$\hat{\rho}(xy) = \rho(y^{-1}x^{-1})^T = [\rho(y^{-1})\rho(x^{-1})]^T$$
$$= \rho(x^{-1})^T\rho(y^{-1})^T = \hat{\rho}(x)\hat{\rho}(y).$$

因而 $\hat{\rho}$ 也是 G 的表示，它叫做表示 ρ 的**逆步表示**.

设 L 是 ρ 的表示模，它在 F 上的基底是 $u_1, \cdots, u_m$，取 F 上具有基底 $v_1, \cdots, v_n$ 的任何空间 $\hat{L}$. 对于 $u = a_1u_1 + \cdots + a_nu_n \in L$ 和 $v = b_1v_1 + \cdots + b_nv_n \in \hat{L}$ 定义纯量积 $u \cdot v$:

$$u \cdot v = a_1b_1 + a_2b_2 + \cdots + a_nb_n \in F.$$

这个纯量积是 $(L, \hat{L})$ 上由 $u_i \cdot v_j = \delta_{ij}$ 决定的双线性函数.

我们用下列等式使 $v_1, \cdots, v_n$ 成为表示 $\hat{\rho}$ 的基底:

$$v_ix = \sum_j \hat{\rho}_{ij}(x)v_j = \sum_j \rho_{ji}(x^{-1})v_j.$$

于是

$$u_ix \cdot v_jx = \sum_{k,s}\rho_{ik}(x)\rho_{sj}(x^{-1})(u_k \cdot v_s)$$

$$= \sum_k \rho_{ik}(x)\rho_{kj}(x^{-1}) = \delta_{ij},$$

因为 $\rho(x)\rho(x^{-1}) = I_n$. 因而对于所有 $u \in L$, $v \in \hat{L}$ 和 $x \in G$，都有 $ux \cdot vx = u \cdot v$，所以当纯量积的两个因子用 G 的同一个元素作用时它的值不变. 对于 $\hat{L}$ 的任何子空间 M'，我们使它对应于 L 的这样的子空间 M，M 由使 $u \cdot v = 0$ 对于所有 $v \in M'$ 都成立的所有 $u \in L$ 组成. 因此 $\dim M' + \dim M = n$，而且这是在 L 和 $\hat{L}$ 的子空间之间的对偶对应. 如果 M' 是 $\hat{L}$ 的表示子模而且 $v \in M'$，则对于 $x \in G$，$vx^{-1} \in M'$，于是 $vx^{-1} \cdot u = 0$ 和 $v \cdot ux = 0$ 对于所有 $v \in M'$ 和 $u \in M$ 都成立，因而 $ux \in M$ 而且 M 是 L 的表示子模. 因此，特别地，$\hat{L}$ 是不

可约的，必要而且只要 L 是不可约的. 如果 ρ 是绝对不可约的 $n\times n$ 表示，则因为 ρ 在 F 上的维数是 n^2，所以 $\hat{\rho}$ 在 F 上的维数也是 n^2，因而它显然是绝对不可约的.

根据定义，$\hat{\hat{\rho}}=\rho$. 又如果 ρ 和 σ 是等价的则存在某个 S，使得对于所有 $x\in G$ 有

$$S^{-1}\rho(x^{-1})S=\sigma(x^{-1}).$$

然后取转置，因而对于所有 $x\in G$ 有

$$S^T\rho(x^{-1})^T S^{T-1}=\sigma(x^{-1})^T,$$

即 $\hat{\rho}$ 和 $\hat{\sigma}$ 也是等价的.

设 r 是 G 的共轭类的个数. 设 $\rho_1,\cdots,\rho_r$ 是 G 在 F 上的绝对不可约表示，这里为了方便起见，我们取 ρ_1 为恒同表示：$\rho_1(x)=1$ 对于所有 $x\in G$. $\left(\text{这对应于幂等元素 } \frac{1}{g}\sum_{x\in G} x.\right)$ 于是 $\hat{\rho}_1=\rho_1,\cdots,\hat{\rho}_r$ 是另一顺序的同一些表示. 同理，设 $C_1,\cdots,C_r$ 是 G 的共轭类，这里为了方便起见，我们取 $C_1=1$ 为单由单位元素组成的类. 同一类 C_i 的元素的逆组成类 C_i'. 因此，$C_1'=C_1,\cdots,C_r'$ 仍然是 C 的共轭类.

设 $\chi(x)$ 是表示 $\rho(x)$ 的特征标，我们把 $\hat{\rho}(x)$ 的特征标记做 $\bar{\chi}(x)$. 这时 $\chi(x)=\mathrm{Tr}\rho(x)$:

$$\bar{\chi}(x)=\mathrm{Tr}\,\rho(x^{-1})^T=\mathrm{Tr}\,\rho(x^{-1})=\chi(x^{-1}),$$

而且我们从定理 16.6.8 知道，在复数域的情形，$\chi(x^{-1})=\overline{\chi(x)}$ 是 $\chi(x)$ 的共轭复数. 因此这个记号与复数域的共轭复数的记号协合. 我们注意到，在复数域上，只有当 ρ 的所有特征标 $\chi(x)$ 都是实数时才有 $\rho=\hat{\rho}$.

设 χ_i^a 是在表示 ρ_a 下的共轭类 C_i 的一个元素的绝对不可约的特征标. 我们把 C_i 中的元素个数记做 h_i. h_i 是元素 $x\in C_i$ 的正规化子的指数，而且设它的阶是 g_i，则 $g_ih_i=g$.

定理 16.6.9. 下列正交关系对于群 G 的绝对不可约的特

征标成立:

$$\sum_{i=1}^{r} \frac{\chi_i^a \overline{\chi_i^b}}{g_i} = \delta_{ab},$$

$$\sum_{a=1}^{r} \overline{\chi_i^a} \chi_j^a = \delta_{ij} g_j.$$

证明. 根据定理 16.6.5，我们有

$$\frac{1}{g} \sum_{x \in G} \chi^a(x) \chi^b(x^{-1}) = \delta_{ab}.$$

但是当 x 和 y 在同一个共轭类 C_i 内时有 $\chi(x) = \chi(y)$，而且这时 x^{-1} 和 y^{-1} 在同一个共轭类 C_i' 内 这时 $\chi^b(x^{-1}) = \overline{\chi^b}(x)$. 因此对于 C_i 中的 x，上面的和式包含 h_i 个等于 $\chi_i^a \overline{\chi_i^b}$ 的项. 因此

$$\sum_{i=1}^{r} \frac{h_i}{g} \chi_i^a \overline{\chi_i^b} = \delta_{ab},$$

即

$$\sum_{i=1}^{r} \frac{\chi_i^a \overline{\chi_i^b}}{g_i} = \delta_{ab}.$$

这说明如果M是这样的矩阵: $M = (m_{ai})$, a, $i = 1, \cdots, r$, 这里 $m_{ai} = \chi_i^a$, 则矩阵

$$M' = (r_{ib}), i, b = 1, \cdots, r$$

这里

$$r_{ib} = \frac{1}{g_i} \overline{\chi_i^b},$$

将使

$$MM' = I_r,$$

因而 M' 是M的逆. 于是还有 $M'M = I_r$, 由此得出

$$\sum_{a=1}^{r} \frac{1}{g_i} \chi_i^a \overline{\chi_j^a} = \delta_{ij},$$

定理中的第二个关系也就得到了.

群环的结构导出特征标之间的进一步的关系. 在分 R_G 为单纯环的直和的分解式

$$R_G = R_1 \boxplus \cdots \boxplus R_a \boxplus \cdots \boxplus R_r$$

中,设 e^a_{ij}, $i, j = 1, \cdots, n$ 是 R_a 的矩阵单位元素,而且 R_a 的单位元素是 $e_a = e^a_{11} + e^a_{22} + \cdots + e^a_{nn}$. 对应于 R_a 的不可约表示 $\rho_a = \rho^a$ 等价于在 R_a 的极小右理想上的表示. 设这个右理想是 $e^a_{11}R$, 它的基底是

$$e^a_{11}, e^a_{12}, \cdots, e^a_{1n}.$$

那么

$$e^a_{1i}x = \sum_j \rho^a_{ij}(x) e^a_{1j}, \quad i = 1, \cdots, n.$$

现在设 $x = x_1 + \cdots + x_a + \cdots + x_r$, 这里 $x_a \in R_a$, 并且

$$x_a = e_a x e_a = e_a x = x e_a.$$

如果

$$x_a = \sum_{i,j} x^a_{ij} e^a_{ij},$$

则 $e^a_{1i}x = e^a_{1i}e_a x = e^a_{1i}x_a$, 而且

$$e^a_{1i} x e^a_{1j} = x^a_{ij} e^a_{1j}.$$

但是根据表示的定义,

$$e^a_{1i} x e^a_{jj} = e^a_{jj}(x) e^a_{1j}.$$

因此,在所有的情形都有 $x^a_{ij} = \rho^a_{ij}(x)$, 所以

$$x_a = \sum_{i,j} \rho^a_{ij}(x) e^a_{ij}.$$

我们记 $C_k = \sum_{x \in C} x$, 因为用同一个记号表示共轭类和作为 R_G 的元素的同类元素的和并不会引起混淆. 于是 $C_1, C_2, \cdots, C_r$ 是 R_G 的中心的基底. 设

$$C_k = C^1_k + \cdots + C^a_k + \cdots + C^r_k,$$

这里 $C_k^a \in R_a$. 那么因为 C_k^a 属于 R_a 的中心 $Z(R_G)$, 它是 e_a 的纯量倍,即

$$C_k^a = u_k^a e_a.$$

但是

$$\mathrm{Tr}\rho^a(C_k^a) = \sum_{x \in C_k} \mathrm{Tr}\rho^a(x),$$

因而 $n_a u_k = h_k \chi_k^a$, 这里 n_a 是 ρ_a 的阶. 因此

$$u_k^a = \frac{h_k \chi_k^a}{n_a},$$

所以

$$C_k^a = \frac{h_k \chi_k^a}{n_a} e_a.$$

R_G 的元素 $C_1, \cdots, C_r$ 作为 $Z(R_G)$ 的元素具有乘法表:

$$C_j C_i = C_i C_j = \sum_k c_{ijk} C_k,$$

这里在特征为零的域 F 上, c_{ijk} 是非负的整数. 因为 $C_i C_j = C_j C_i$ 不包含负项.

因为 R_G 是单纯环 R_a 的直和. 分支 C_i^a 将满足 C_i 所满足的同样关系. 因此:

定理 16.6.10.

$$C_i^a C_j^a = C_j^a C_i^a = \sum_k c_{ijk} C_k^a, \quad a = 1, \cdots, r$$

而且

$$\frac{h_i \chi_i^a}{n_a} \frac{h_j \chi_j^a}{n_a} = \sum_k c_{ijk} \frac{h_k \chi_k^a}{n_a}, \quad a = 1, \cdots, r.$$

在定理 16.6.4 的证明中指出过 $n\lambda = 1$, 这里 $n = n_a$ 是绝对不可约表示的阶. 因此在定理 16.6.10 中用 n_a 除是许可的.

给了域 F 上的两个线性空间 L 和 M, 我们用下列方式定

义它们的张量乘积 $L \times M$：如果 $u_1, \cdots, u_m$ 是 L 的基底，$v_1, \cdots, v_n$ 是 M 的基底，则 $L \times M$ 是 F 上具有基底 $u_i v_j$，$i = 1, \cdots, m$，$j = 1, \cdots, n$ 的线性空间．对于

$$u = a_1 u_1 + \cdots + a_m u_m \in L$$

和

$$v = b_1 v_1 + \cdots + b_n v_n \in M,$$

我们定义乘积 $uv = \sum_{i,j} a_i b_j u_i v_j$ 为 $L \times M$ 的元素．可以验证，L 或 M 的基底变换对应于 $L \times M$ 的基底变换．

如果 L 是群 G 的表示 ρ 的 F-G 模，而且 M 是 G 的表示 σ 的 F-G 模，则我们定义表示 ρ 和 σ 的克朗耐克乘积 $\rho \times \sigma$ 为 G 在 $L \times M$ 上的表示，它由下列等式决定：

$(uv)x = (ux)(vx)$，对于所有 $u \in L$，$v \in M$，$x \in G$，

因此如果 ρ_1 等价于 ρ 而且 σ_1 等价于 σ，则 $\rho_1 \times \sigma_1$ 等价于 $\rho \times \sigma$，因为这对应于 L 和 M 的基底变换．

定理 16.6.11. 如果 ρ 和 σ 是 G 的表示，它们的特征标分别是 χ 和 ψ，又如果 ϕ 是 $\rho \times \sigma$ 的特征标，则对于每个 $x \in G$，我们有 $\phi(x) = \chi(x)\psi(x)$.

证明. 如果

$$u_i x = \sum_j \rho_{ij}(x) u_j, \quad i = 1, \cdots, m,$$

$$v_i x = \sum_j \sigma_{ij}(x) v_j, \quad i = 1, \cdots, n,$$

则

$$\chi(x) = \sum_i \rho_{ii}(x), \quad \psi(x) = \sum_i \sigma_{ii}(x).$$

但是因为

$$(u_i v_j)x = \sum_{k,t} [\rho_{ik}(x) u_k][\sigma_{jt}(x) v_t];$$

所以

$$\phi(x) = \sum_{i,j} \rho_{ii}(x)\sigma_{jj}(x)$$
$$= \left[\sum_i \rho_{ii}(x)\right]\left[\sum_j \sigma_{jj}(x)\right] = \chi(x)\phi(x).$$

从定义知道张量乘积和克朗耐克乘积是可交换的和可结合的. 因此如果 ρ_a 和 ρ_b 是G的绝对不可约表示,则

$$\rho_b \times \rho_a = \rho_a \times \rho_b = \sum_c g_{abc}\rho_c,$$

(这里 g_{abc} 是非负整数) 是分 $\rho_a \times \rho_b$ 为具有系数 g_{abc} 的不可约表示 ρ_c 的直和的分解式. 同样的关系对于特征标也成立. 我们写成一个定理.

定理 16.6.12. 群G的绝对不可约表示满足关系

$$\chi_i^a\chi_i^b = \sum_c g_{abc}\chi_i^c,$$

这里 g_{abc} 是非负整数, 这些数是一个可交换的和可结合的代数的乘法常数.

我们把已经得出的特征标之间的关系总结一下, 设 $C_1 = 1, C_2, \cdots, C_r$ 是G的共轭类, ρ_1 是恒同表示, $\rho_2, \cdots, \rho_r$ 是绝对不可约表示, χ_i^a 是第 a 个表示中的第 i 个共轭类的特征标:

	$C_1 \cdots$	$C_i \cdots$	C_r
ρ_1	$\chi_1^1 \cdots$	$\chi_i^1 \cdots$	χ_r^1
	$\cdots\cdots$	$\cdots\cdots$	$\cdots$
ρ_a	$\chi_1^a \cdots$	$\chi_i^a \cdots$	χ_r^a
	$\cdots\cdots$	$\cdots\cdots$	$\cdots$
ρ_r	$\chi_1^r \cdots$	$\chi_i^r \cdots$	χ_r^r

这时我们有 $g_ih_i = g$, 这里 h_i 是共轭类 C_i 的元素的个数.

下列正交关系成立:

1) 在行之间;

$$\sum_{i=1}^{r}\frac{\chi_i^a\overline{\chi_i^b}}{g_i}=\delta_{ab}.$$

2）在列之间：

$$\sum_{a=1}^{r}\chi_i^a\chi_j^a=\delta_{ij}g_i.$$

3）在每一行内：

$$\frac{h_i\chi_i^a}{n_a}\frac{h_j\chi_j^a}{n_a}=\sum_k c_{ijk}\frac{h_k\chi_k^a}{n_a}.$$

4）在每一列内：

$$\chi_i^a\chi_i^b=\sum_c g_{abc}\chi_i^c.$$

这里 c_{ijk} 和 g_{abc} 是非负整数，它们是可交换和可结合的代数的乘法常数.

群 G 的每个作为置换群 $\pi(G)$ 的表示也可以看做矩阵表示，因为如果

$$\pi(x)=\begin{pmatrix}u_1 & \cdots u_n\\ u_{i_1} & \cdots u_{i_n}\end{pmatrix}$$

对于 $x\in G$，则可以把它看作基底 $u_1,\cdots,u_n$ 上的表示 ρ，这里

$$u_jx=u_{i_j}.$$

于是 $\chi(x)$ 就是在 $\pi(x)$ 下不变的文字的个数.

定理 16.6.13. 在 g 阶群 G 的置换表示 $\pi(G)$ 中，

$$\sum_{x\in G}\chi(x)=kg,$$

这里 k 是传递组的个数. 这时作为矩阵表示的表示恰好包含恒同表示 k 次.

证明. 设 $n_1,n_2,\cdots,n_k$ 是在 k 个传递组内的元素个数. 那么不变第 i 个传递组的元素 a_i 的子群 H_i 的指数是 n_i，因而它的阶是 g/n_i. 因此文字 a_i 在 G 的元素作用下有

g/n_i 次不变.于是第 i 个传递组的文字不变的次数是 $n_i \cdot g/n_i = g$. 因此 k 个传递组的任何文字不变的次数是 kg, 即

$$\sum_{x \in G} \chi(x) = kg.$$

如果 $\chi = \sum_{a} m_a \chi^a$ 把 χ 表成绝对不可约特征标的和，则根据定理 16.6.5 的推论, $\sum_{x \in G} \chi(x) = m_1 g$. 因此已知表示包含恒同表示 $m_1 = k$ 次.

定理 16.6.14. 如果 χ 是传递的置换群 G 的特征标，则 $\sum_{x \in G} \chi^2(x) = tg$, 这里 t 是不变一个文字的子群 H 的传递组的个数. t 也是 G 内的二重傍系 HxH 的个数.

证明. 设 G 是 $1, 2, \cdots, n$ 上的传递的置换群. 设 H_i 是不变 i $(i = 1, \cdots, n)$ 的子群. 我们可以取 $H = H_1$, 因为所有 H_i 都是共轭的. 设 h 是 H 的阶. 那么根据前面的定理

$$\sum_{x \in H_i} \chi(x) = th.$$

因此

$$\sum_{i} \sum_{x \in H_i} \chi(x) = tnh = tg.$$

在左边我们对于包含 x 的每个 H_i 都计算一次 $\chi(x)$. 但是因为 x 不变 $\chi(x)$ 个文字，所以它包含在 $\chi(x)$ 个不同的 H_i 内.(当 x 变动全体文字时这个数是零.)因此

$$tg = \sum_{i} \sum_{x \in H_i} \chi(x) = \sum_{x \in G} \chi^2(x).$$

容易证明 t 是 G 内的二重傍系 HxH 的个数. 事实上，设

$$G = H + Hx_2 + \cdots + Hx_n,$$

这里 H 是不变 1 的子群而且 $x_i = (1, i, \cdots)$, $i = 2, \cdots, n$.

那么如果 $Hx_iH = Hx_jH$，则就有 $x_i = h_1x_jh_2$，这里 $h_1, h_2 \in H$. 这时元素 h_2 必定把 j 变成 i，因而 i 和 j 属于H的同一个传递组. 反之，假定 i 和 j 属于H的同一个传递组. 那么存在某个 $h_2 \in H$，h_2 把 j 变成 i，x_jh_2 把 1 变成 i，因而 $x_jh_2 \in Hx_i$，于是 $x_i = h_1x_jh_2$ 而且 $Hx_iH = Hx_jH$. 总之H的每个二重傍系是 Hx_iH 中的一个. 因此二重傍系 HxH 的个数恰好等于H内的传递组的个数.

定理 16.6.15. 群 G 在复数域上的二重传递的置换表示是恒同表示和一个绝对不可约表示的和.

证明. 对于二重传递表示，

$$\Sigma\chi^2(x) = 2g,$$

因为不变文字 1 的子群H恰好有两个传递组：1 和包含其余元素的传递组. 因为 $\chi(x)$ 是实数，我们可以改写成

$$\sum_{x\in G}\chi(x)\overline{\chi(x)} = 2g.$$

但是如果 $\chi = \sum_a c_a\chi^a$ 是把 χ 表成绝对不可约特征标的和，则根据正交关系有

$$\sum_{x\in G}\chi(x)\overline{\chi(x)} = \sum_x\left[\sum_a c_a\chi^a(x)\right] \times\left[\sum_a c_a\overline{\chi^a(x)}\right] = g\sum_a c_a^2.$$

因此 $\sum_a c_a^2 = 2$，于是 $c_1 = 1$（这是已经知道的）而且恰好有一个 $c_a = 1$.

16.7. 非本原表示

设给了群G的表示模 M，它是子空间 $M_1, M_2, \cdots, M_n$

的直和，而且在这些子空间上表示是传递的和非本原的．这意思是说：

1）对于任何 M_i 和 M_j，存在 $x\in G$，使得

$$M_i x = M_j.$$

2）对于每个 M_i 和每个 $x\in G$，存在 M_j，使得

$$M_i x = M_j.$$

其中第一个是传递性质；第二个是非本原性质．

取特殊的子空间 M_1．使 $M_1 x = M_1$ 的全体 x 的集合当然包含 $x=1$，因而不是空的，它显然是 G 的子群 H．因而对于 $h\in H$，

$$M_1 h = M_1,$$

所以 M_1 是 H 的表示模．如果 $b_i\in G$ 是使

$$M_1 b_i = M_i$$

的元素，则使 $M_1 x = M_i$ 的元素 x 是傍系 Hb_i 的元素．因而有

$$G = H + Hb_2 + Hb_3 + \cdots + Hb_n,$$

这里

$$M_1(hb_i) = M_i,\ i = 1,\cdots,n,$$

而且我们使子空间对应于 H 的左傍系．如果 x 使得

$$M_i x = M_i,$$

则

$$M_1 b_i x = M_1 b_i,$$

而且

$$M_1 b_i x b_i^{-1} = M_1,$$

因而 $b_i x b_i^{-1}\in H$ 或 $x\in b_i^{-1}Hb_i$，后者是 H 的共轭子群，最后，如果

$$M_i x = M_j,$$

则

$$x \in b_i^{-1}Hb_j.$$

设 ρ_1 是对应于 M_1 的基底 $v_1, \cdots, v_m$ 的 H 的表示. 那么我们可以取 $v_1b_i, \cdots, v_mb_i$ 作为 M_i 的基底. 于是对于任意 $x \in G$，我们有

$$M_1x = M_{j_1}, \cdots, M_ix = M_{j_i}, \cdots, M_nx = M_{j_n}.$$

这里 $M_{j_1}, \cdots, M_{j_n}$ 是 $M_1, \cdots, M_n$ 的置换，因为用 x^{-1} 作用于它们将回过来得出 $M_1, \cdots, M_n$，这时如果 $M_ix = M_j$ $(j = j_i)$，则 $x \in b_i^{-1}Hb_i$，或 $b_ixb_j^{-1} = h_{ij} \in H$. 因此，当取 v_kb_i，$k = 1, \cdots, m$ 作为 M_i 的基底时，我们有

$$v_kb_i \cdot x = (v_k \cdot h_{ij})b_j, \ k = 1, \cdots, m.$$

换句话说，表示的这一部分完全由元素 h_{ij} 在 M_1 上的表示决定：

$$v_k(b_ixb_j^{-1}) = v_kh_{ij}.$$

因此，

$$\rho(x) = (\rho_1(b_ixb_j^{-1})), \ i, j = 1, \cdots, n,$$

这里当 $y \notin H$ 时规定 $\rho_1(y) = 0$. 于是 $\rho(x)$ 的阶是 mn，它由 n^2 个 m 阶矩阵拼成. 因此，在子空间 $M_1, \cdots, M_n$ 上传递的和非本原的每个表示由 G 内一个指数 n 的子群的表示 ρ_1 决定. 逆命题也成立. 设 ρ_1 是 H 的任何表示，这里

$$G = H + Hb_2 + \cdots + Hb_n.$$

然后定义.

$$\rho(x) = (\rho_1(b_ixb_j^{-1})), \ i, j = 1, \cdots, n,$$

这里当 $y \notin H$ 时规定 $\rho(y) = 0$. 那么利用矩阵的分块乘法就有

$$\begin{aligned}\rho(x)\rho(y) &= (\rho_1(b_ixb_j^{-1}))(\rho_1(b_kyb_t^{-1}))\\ &= (\rho_1(b_ixb_j^{-1}))(\rho_1(b_jyb_t^{-1}))\\ &= (\rho_1(b_ixyb_t^{-1})) = \rho(xy),\end{aligned}$$

而且显然有

$$\rho(1)=(\rho_1(b_i1b_j^{-1}))=(\rho_1(1))=I.$$

因而 $\rho(x)$ 是G的表示.

定理 16.7.1. 给了群G的子群H的m阶表示 ρ_1. 如果

$$G=H+Hb_2+\cdots+Hb_n,$$

则

$$\rho(x)=(\rho_1(b_ixb_j^{-1})),\ i,j=1,\cdots,n,$$

这里在 $y\notin H$ 时规定$\rho_1(y)=0$,是G在模M上的 mn 阶表示,这时M具有分别对应于 $H, Hb_2, \cdots, Hb_n$ 的子空间 $M_1, M_2, \cdots, M_n$. ρ 在 $M_1, \cdots, M_n$ 上是传递的和非本原的. 反之,在模的子空间上传递的和非本原的任何表示都是这种类型的.

证明. 如果 $u_1, \cdots, u_m, \cdots, u_{mn}$ 是定理中的 ρ 的表示模M的基底,则 $u_1, \cdots, u_m$ 是H的对应于 ρ_1 的基底,而且 $u_{m(i-1)+j}=u_jb_i$, $i=1,\cdots,n$. 由此推出具有基底 $u_1, \cdots, u_{mn}$ 的模M有子空间 $M_1, \cdots, M_n$, 而且 ρ 在这些子空间上是传递的和非本原的. 我们说G的表示ρ由H的表示 ρ_1 导出.

推论 16.7.1. 由H的表示 ρ_1 导出的G的表示 ρ 不依赖于H在G内的傍系代表的选取.

这是因为更换傍系代表并不改变子空间 $M_1, \cdots, M_n$ 而只不过改变它们的基底.

定理 16.7.2. 设χ是由H的表示 ρ_1 导出的G的表示ρ的特征标,而且 ρ_1 的特征标是 χ_1. 设x属于G的共轭类 C_j, 后者有 h_j 个元素,而且设 $g=g_jh_j$, 这里 g 是G的阶. 再设H的阶是 h. 那么

$$\chi(x)=\frac{g_j}{h}\sum_{z\in C_j\cap H}\chi_1(z).$$

证明.

$$\chi(x) = \sum_i \chi_1(b_i x b_i^{-1}),$$

这里当 $w \notin H$ 时规定 $\chi_1(w) = 0$. 于是

$$\chi(x) = \frac{1}{h} \sum_{y \in G} \chi_1(yxy^{-1}),$$

因为对于 Hb_i 的每个元素 y，值 $\chi_1(yxy^{-1})$ 都等于 $\chi_1(b_i x b_i^{-1})$. 于是当 y 遍历 G 时，yxy^{-1} 遍历 C_j 而且对于每个 $z \in C_j$ 都恰好重复 g_j 次. 因此

$$\sum_{y \in G} \chi_1(yxy^{-1}) = g_j \sum_{z \in C_j \cap H} \chi_1(z),$$

这就证明了定理.

定理 16.7.3（互易定理）. 设 ρ 和 ρ_1 分别是群 G 和子群 H 在特征为零的域上的绝对不可约表示. 那么 ρ_1 在限定于 H 上的 ρ 中出现的次数与 ρ 在由 ρ_1 导出的 G 的表示 ρ^* 中出现的次数相同.

证明. 设 $\chi = \chi^a$ 是 ρ 的特征标，又 $\chi_1 = \chi_1^c$ 是 ρ_1 的特征标. 再设 χ^* 是 ρ^* 的特征标，$\chi^* = \sum_b m_b \chi^b$，这里 χ^b 是 G 的不可约特征标. 在限定于 H 时，设

$$\chi = \chi^a = \sum_d n_d \chi_1^d,$$

这里 χ_1^d 是 H 的不可约特征标. 于是 ρ 在 ρ^* 内的次数是 m_a，而 ρ_1 在限定于 H 的 ρ 内的次数是 n_c. 根据上面的定理，

$$\frac{1}{g_j} \chi_j^* = \frac{1}{g_j} \sum_b m_b \chi_j^b = \frac{1}{h} \sum_{z \in C_j \cap H} \chi_j^c(z).$$

这时规定对于空集取的和式是零. 用 $\overline{\chi_j^a}$ 乘这个式子而且对 j 求和，我们得出

$$\sum_{j,b} m_b \frac{\overline{\chi}_j^a \chi_j^b}{g_j} = \frac{1}{h} \sum_j \overline{\chi}_j^a \sum_{z \in C_j \cap H} \chi_1^c(z),$$

因而利用G内和H内的正交关系，

$$m_a = \frac{1}{h} \sum_{d,j} n_d \overline{\chi}_{1,j}^d \sum_{z \in C_j \cap H} \chi_1^c(z)$$

$$= \frac{1}{h} \sum_{d, z \in H} n_d \overline{\chi}_1^d(z) \chi_1^c(z)$$

$$= \frac{1}{h} h n_c = n_c,$$

这就是定理的结论.

16.8. 特征标理论的若干应用

在整个这节中我们假定所牵涉的域F是复数域，虽然读者容易看出，对于特征不整除被表示的群G的阶的所有的域，一系列的结果也成立.

首先需要关于代数数的若干事实[1]. 代数数 θ 是指下列首项系数为 1 的多项式的根 $x = \theta$:

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0,$$

这里 $a_1, \cdots, a_n$ 是有理数. 当多项式的系数 $a_1, \cdots, a_n$ 是有理整数时，它的根 θ 叫做代数整数.

定理 16.8.1. 作为代数整数的有理数是有理整数.

证明. 假定 $\theta = r/s$ 是最简分数而且满足

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0,$$

这里 $a_1, \cdots, a_n$ 是整数. 那么

$$r^n = -s(a_1 r^{n-1} + a_2 s r^{n-2} + \cdots + a_n s^{n-1}).$$

因此整除 s 的任何素数必定整除 r^n，因而也整除 r. 当 r/s

1) 这些事实包含在 Birkhoff and MacLane [1] 第 410—422 页内.

是最简分数而且 $s \neq 1$ 时这不可能成立．因此 $s = 1$，所以 $\theta = r$ 是有理整数．

定理 16.8.2. 代数数组成域．两个代数整数的和以及乘积都是代数整数．

证明. 设 θ 是满足 $x^n + a_1x^{n-1} + \cdots + a_n = 0$ 的代数数，ϕ 是满足 $x^m + b_1x^{m-1} + \cdots + b_m = 0$ 的代数数．设

$$v_{i,j} = \theta^i\phi^j, i = 0, \cdots, n-1, j = 0, \cdots, m-1.$$

那么

$$\theta v_{i,j} = v_{i+1,j} \text{ 对于 } i = 0, \cdots, n-2,$$

而且

$$\theta v_{n-1,j} = -a_1v_{n-1,j} - \cdots - a_nv_{0j}.$$

同理，

$$\phi v_{i,j} = v_{i,j+1} \text{ 对于 } j = 0, \cdots, m-2,$$

而且

$$\phi v_{i,m-1} = -b_1v_{i,m-1} - \cdots - b_mv_{i0}.$$

引理 16.8.1. 如果 $y_1, \cdots, y_N$ 是不全为零的数而且 z 是使下列等式成立的数：

$$zy_i = \sum_j a_{ij}y_j, i = 1, \cdots, N,$$

这里 a_{ij} 都是有理数，则 z 是代数数．又如果 a_{ij} 是整数，则 z 是代数整数．

证明. 定理的假设给出一组方程：

$$\begin{aligned}
(a_{11} - z)y_1 + a_{12}y_2 + \cdots + a_{1N}y_N &= 0,\\
a_{21}y_1 + (a_{22} - z)y_2 + \cdots + a_{2N}y_N &= 0,\\
\cdots\cdots\cdots&\\
a_{N1}y_1 + a_{N2}y_2 + \cdots + (a_{NN} - z)y_N &= 0,
\end{aligned}$$

它们作为 y_i 的线性方程，具有不全是零的解 $y_1, \cdots, y_N$．因此系数行列式必定是零：

$$\begin{vmatrix} a_{11}-z, & a_{12}, & \cdots, & a_{1N} \\ a_{21}, & a_{22}-z, & \cdots, & a_{2N} \\ \cdots & \cdots & \cdots & \cdots \\ a_{N1}, & a_{N2}, & \cdots, & a_{NN}-z \end{vmatrix} = 0.$$

它展开以后是

$$(-1)^N z^N + p_1 z^{N-1} + \cdots + p_N = 0,$$

这里系数 p_j 都是 a_i 的整系数多项式. 因此如果 a_i 是有理数，则 z 是代数数,而如果 a_i 是整数,则 z 是代数整数.

我们可以利用这个引理来证明定理. 我们排除了当 θ 或 ϕ 是 0 的显然情形. 我们取 $y_1, \cdots, y_N$ 为 v_{ij}, 而且因为 $v_{00}=1$, 这些 v_{ij} 不全是零. 然后取 z 为 $\theta+\phi$ 或 $\theta\phi$. 于是引理中的 a_{ij} 是 $a_1, \cdots, a_n$ 和 $b_1, \cdots, b_m$ 的整系数多项式. 因此 $z=\theta+\phi$ 和 $z=\theta\phi$ 是代数数,而且如果 $a_1, \cdots, a_n$ 和 $b_1, \cdots, b_m$ 是整数, 则 $\theta+\phi$ 和 $\theta\phi$ 是代数整数. 总之, 代数数的和以及乘积是代数数,代数整数的和以及乘积是代数整数. 最后, 设 $\theta \neq 0$ 是满足 $z^n + a_1 z^{n-1} + \cdots + a_n = 0$ 的代数数,必要时用 z 的方幂除,可以假定常数项 $a_n \neq 0$. 于是

$$w^n + \frac{a_{n-1}}{a_n} w^{n-1} + \cdots + \frac{1}{a_n} = 0$$

是 $1/\theta$ 所满足的方程. 显然 $-\theta$ 满足 $z^n - a_1 z^{n-1} + \cdots + (-1)^n a_n = 0$. 因此代数整数组成整区[1)]而代数数组成域.

定理 16.8.3. 每个特征标 $\chi(x)$ 都是代数整数. 定理 16.6.10 中的数 $h_i \chi_i^a / n_a$ 是代数整数.

证明. m 次单位根满足 $x^m - 1 = 0$, 因而它是代数整数. 根据定理 16.6.8, 每个特征标 $\chi(x)$ 是单位根的和, 因而它是代数整数. 因为定理 16.6.10 中的 c_{ijk} 是整数, 所以我

---

1) 即无零因子的交换环. ——俄译者注

们可以取

$$\frac{h_i\chi_i^a}{n_a}=\eta_i^a,\ i=1,\cdots,r$$

作为引理 16.8.1 中的 y_i 而且取其中任何一个作为 z,就可以利用这个引理得出 η_i^a 是代数整数的结果.

定理 16.8.4. 有限群 G 的绝对不可约表示的阶 n_a 整除 G 的阶 g.

证明. 根据正交关系,

$$\sum_{i=1}^{r}\frac{\chi_i^a\overline{\chi}_i^a}{g_i}=1.$$

因为 $g_ih_i=g$, 这可以改写成

$$\sum_{i=1}^{r}\frac{\chi_i^a h_i\overline{\chi}_i^a}{g}=1,$$

或

$$\sum_{i=1}^{r}\frac{h_i\chi_i^a}{n_a}\chi_i^a=\frac{g}{n_a}.$$

上述等式左边是代数数的乘积之和. 因此 g/n_a 是代数数, 然而它又是有理数,所以它是有理整数. 因而 n_a 整除 g.

为了应用代数数, 我们需要关于对称函数的一点知识. 展开

$$(z-x_1)(z-x_2)\cdots(z-x_n)$$
$$=z^n-E_1z^{n-1}+E_2z^{n-2}+\cdots+(-1)^nE_n,$$

我们有

$$E_1=\Sigma x_i,$$
$$E_2=\Sigma x_ix_j,$$
$$\cdots\cdots\cdots$$
$$E_r=\Sigma x_{i_1}x_{i_2}\cdots x_{i_r},$$
$$\cdots\cdots\cdots$$

$$E_n = x_1x_2\cdots x_n.$$

这时 $E_1, \cdots, E_n$ 在 $x_1, \cdots, x_n$ 的任何置换下显然不变，它们叫做 $x_1, \cdots, x_n$ 的初等对称函数. 域 F 上的多项式 $P(x_1, \cdots, x_n)$ 叫做对称函数，假如它在 $x_1, \cdots, x_n$ 的置换的整个对称群下不变.

定理 16.8.5. 每个对称函数 $P(x_1, \cdots, x_n)$ 是初等对称函数 $E_1, \cdots, E_n$ 的多项式 $Q(E_1, \cdots, E_n)$，而且 Q 的系数是 P 的系数的整多项式.

证明. 如果 P 是对称的，则它的每一次数的同次项本身也组成对称函数. 当次数为 1 时定理显然成立，因为这时的对称函数只有 cE_1, $c \in F$. 其次，P 是一些对称多项式的和，这种对称多项式由下列形式的单独一项决定:

$$c(x_1\cdots x_r)^a(x_{r+1}\cdots x_{r+s})^b\cdots(x_{u+1}\cdots x_{u+v})^t,$$

这里方次数 $a > b > \cdots > t$ 是严格递降的. 只要对于下列对称和式证明定理就成了:

$$K = \Sigma(x_1\cdots x_r)^a(x_{r+1}\cdots x_{r+s})^b\cdots(x_{u+1}\cdots x_{u+v})^t,$$

这里 $a > b > \cdots > t$. 我们对下列各数施行归纳法: (1) K 的次数; (2) a 的值; (3) r 的值. 如果 $x_1, \cdots, x_n$ 在每一项里出现，我们把 E_n 括出，剩下的因子是较低次的对称多项式. 因此可以假定 $u + v < n$. 如果 $a = 1$，则 $K = E_r$. 在 $a \neq 1$ 的情形，考虑

$$\Sigma x_1\cdots x_r \cdot \Sigma(x_1\cdots x_r)^{a-1}(x_{r+1}\cdots x_{r+s})^b$$
$$\cdots(x_{u+1}\cdots x_{u+v})^t = E_r \cdot K^*.$$

于是 $E_r \cdot K^* = K +$ 其他的项. 在归纳法中 K^* 和其他的项都处在 K 之前，因而定理证明了.

以代数数 θ 为根的最低次有理系数多项式叫做 θ 的极小多项式. 如果

$$f(x) = x^n + a_1x^{n-1} + \cdots + a_n$$

是θ的极小多项式，则它是以θ为根的任何有理系数多项式$h(x)$的因式．又如果

$$f(x)=(x-\theta_1)(x-\theta_2)\cdots(x-\theta_n),$$

这里$\theta_1=\theta$，则我们说θ_1，$\cdots$，θ_n是θ的共轭数．因此θ的共轭数也满足以θ为根的任何有理系数多项式．因此如果θ是代数整数，则它的共轭数也是代数整数，因而θ的极小多项式的系数作为θ的共轭数的对称函数，都是代数整数，因此是有理整数．

在研究表示时，我们常常要处理单位根．m次本原单位根是$\omega=\exp(2\pi_i/m)$和方幂ω^j，这里$(j,m)=1$．ω和其他m次本原单位根满足$x^m-1=0$，而不满足方程$x^r-1=0$，$0<r<m$．其他m次单位根满足方程$x^d-1=0$，这里d遍历m的约数．从x^m-1约去它与x^d-1的所有公共因子，留下的有理多项式$f(x)$恰好以全体m次本原单位根作为它的根．因此，

$$f(x)=\prod_j(x-\omega^j),\ (j,m)=1,$$

而且$f(x)$是$\phi(m)$次的有理整系数多项式，$\phi(m)$是欧拉ϕ函数．$f(x)$事实上是不可约的，但是没有比我们这里能证明的为多的代数数理论的知识，这一点是很难证明的．我们只需要知道m次本原根的对称函数是有理整数．

定理 16.8.6. 设ρ_a是群G的n阶绝对不可约表示，而且存在共轭类C_i使$(h_i,n)=1$．那么或者(1) $\chi_i^a=0$，或者(2) $\chi_i^a=n\omega$，这里ω是单位根，而且C_i的像属于ρ_a的中心．

证明. 对于特殊的$x\in C_i$，我们可以作ρ_a的变形，使得$\rho_a(x)$具有对角形式．如果x的全体特征根[1]都等于某个

1）或者叫做特征值．——译者

m 次单位根 ω，则

$$\rho_a(x) = \omega I_n,\quad \chi(x) = n\omega,$$

而且 x 的像属于 ρ_a 的中心. 这是定理中的第二种情形. 因此我们必须证明，如果 x 的特征根不全相等，则在定理的假设下，$\chi(x) = 0$. 在这种情形下，χ 的阶是 m，$\chi_i^a = \chi(x) = \omega^{e_1} + \cdots + \omega^{e_n}$ 而且 $|\chi_i^a| < n$，因为 ω^{e_i} 并非全部相同. 这时

$$\frac{h_i\chi_i^a}{n}$$

是代数整数，而且因为 $(h_i, n) = 1$，所以存在整数 r 和 s，使得 $rh_i + sn = 1$. 因此

$$r\left(\frac{h_i\chi_i^a}{n}\right) + s\cdot\chi_i^a = \frac{\chi_i^a}{n}$$

是代数整数. 于是

$$\left|\frac{\chi_i^a}{n}\right| < 1,$$

而且

$$\xi = \frac{\chi_i^a}{n} = \frac{\omega^{e_1} + \cdots + \omega^{e_n}}{n}.$$

把 ω 换成它的共轭数 ω^j，我们得到多项式:

$$\prod_{(j,m)=1} [z - \omega^j],$$

它的系数是共轭根的对称函数，因此是有理数. 于是 ξ 的共轭数出现在下列形式的数中:

$$\frac{\omega^{je_1} + \cdots + \omega^{je_n}}{n},$$

因而对于 ξ 的每个共轭数 $\xi^{(i)}$，我们有 $|\xi^{(i)}| \leqslant 1$，而且每个共轭数都是代数整数. 因为 $|\xi| = |\xi^{(1)}| < 1$，所以 $|\xi^{(1)}\cdots\xi^{(s)}| < 1$，这里 $\xi^{(1)}, \cdots, \xi^{(s)}$ 是 ξ 的所有共轭数. 乘积 $\xi^{(1)}\cdots$

$\xi^{(s)}$必定是有理整数,因而必定是0. 因此$\xi^{(1)}\cdots\xi^{(s)}=0$. 于是至少有一个共轭数是0. 但是0是它自己的唯一的共轭数,所以$\xi=\xi^{(1)}=0$,即

$$\xi=\frac{\chi_i^a}{n}=0.$$

因而$\chi_i^a=0$,这就是我们所要证明的.

定理 16.8.7.[1] (1)如果G的共轭类C_i的元素数h_i是素数的方幂,则G不是单纯群. 确切地说,存在G的同态像,它的中心包含着C_i的元素的像. (2)对于素数p和q,p^aq^b阶的群是可解的.

证明. (1)设$n_1=1, n_2, \cdots, n_r$是G的绝对不可约表示的阶. 设$h_i=p^s$是C_i中的元素数. 对于G的正则表示,我们有$\chi(x)=0$对于$x\in C_i$(因为$x\neq 1$);又根据正则表示的分解式:

$$\chi(x)=\sum_{a=1}^{r} n_a\chi_i^a.$$

这里$n_1\chi_i^1=1$. 对于其余的项,如果$p|n_a$,则根据定理16.8.6,或者$\chi_i^a=0$,或者C_i的像属于同态像$\rho_a(G)$的中心. 但是如果在$p\nmid n$时有$\chi_i^a=0$,则

$$0=1+\sum_{a=2}^{r} n_a\chi_i^a=1+p\alpha,$$

这里α是代数整数. 这将使$-(1/p)$成为代数整数而出现矛盾. 因此对于某个ρ_a,C_i的像属于$\rho_a(G)$的中心.

(2)设G是p^aq^b阶的群. 我们对这种群的阶施行归纳法. p群是可解的. 属于西罗q子群的中心的元素或者属于G的中心,或者它的共轭元素数是p的方幂. 不论那种情形

1) 参看 W. Burnside [2], 第 322—323 页.

G都有正规真子群H，而且根据归纳假设H和G/H都是可解的，所以G是可解的。

定理 16.8.8（弗格贝尼）. 如果G是传递的n次置换群，它的不是单位元素的置换最多保持一个文字不变，则G的变动所有文字的置换和单位元素共同组成n阶的正规子群.

证明. 设G置换$1, 2, \cdots, n$而且H_i是不变i的子群. 那么根据假设，$H_i \cap H_j = 1$对于$i \neq j$. 如果$H = H_1$具有阶h. 则所有H_i都有阶h，因而属于所有H_i的元素$x \neq 1$的总数是$(h-1)n$. 因为$[G:H] = n$，所以G的阶是hn. 因此在G中恰好留下n个其他元素，包括单位元素和$n-1$个变动全体文字的元素.

设ϕ是H的绝对不可约特征标，ϕ'是它所导出的G的特征标. 群G可以看作自己的表示，而且这时它有特征标$\theta_1 = \phi_1'$，这里ϕ_1是H的恒同特征标. 根据定理 16.6.15，θ_1是G的恒同特征标和另一个特征标的和. 设r_G是G的正则表示的特征标. 令$\omega = r_G - h\theta$. 我们的定理将取决于证明ω是G的特征标. 在下面关于特征标的表中设$x \neq 1$是H的典型元素，y是变动全体文字的典型元素.

	1	x	y
ϕ'	mn,	$\phi(x)$,	0
θ	$n-1$,	0,	-1
r_G	nh,	0,	0
ω	h,	0,	h

这里m是ϕ的阶，ϕ', θ, r_G都是已知特征标，如果ω是特征标，则因为$\omega(1) = h$，所以它是h阶表示的特征标. 因为$\omega(y) = h$, $\omega(x) = 0$，所以每个y都由单位元素表示，而每个x都不如此. 因此ω是群G的这样的表示，它的核由1和

变动全体文字的元素 y 组成．作为同态的核，单位元素和变动全体文字的 $n-1$ 个元素组成 G 的正规子群．

我们再来证明 ω 是特征标．设 s 是 H 中的共轭类的个数，而且 ψ^a, $a=1,\cdots,s$ 是 H 的 m_a 阶绝对不可约特征标．那么

$$r_H=\sum_{a=1}^{s} m_a\psi_a.$$

但是 $r_G=(r_H)'$ 而且 $h=\sum_a m_a^2$．因此

$$\omega=\sum_a m_a[(\psi^a)-m_a\theta].$$

因此只要证明 $\psi'-m\theta$ 对于任意 $\psi=\psi^a$ 和 $m=m_a$ 都是 G 的特征标．

我们来计算纯量积

$$\begin{aligned}&(\psi'-m\theta,\psi'-m\theta)\\&=(\psi',\psi')-2m(\psi',\theta)+m^2(\theta,\theta).\end{aligned}$$

因为 $g=nh$，所以根据前面关于特征标的表，

$$\begin{aligned}(\psi',\psi')&=\frac{m^2n}{h}+\frac{1}{nh}\sum_x\psi(x)\overline{\psi(x)}\\&=\frac{m^2n}{h}+\frac{1}{h}\sum_{\substack{x\in H\\x\neq 1}}\psi(x)\overline{\psi(x)}.\end{aligned}$$

但是

$$\sum_{x\in H}\psi(x)\overline{\psi(x)}=h,$$

因而

$$(\psi',\ \psi')=[m^2n+(h-m^2)]/h.$$

同理，根据上面的表，$(\psi',\theta)=m(n-1)/h$，而且

$$(\theta,\theta)=[(n-1)^2+(n-1)]/nh=(n-1)/h.$$

因此

$$(\psi' - m\theta, \psi' - m\theta) = 1.$$

然而 $\psi' - m\theta$ 在任何情况下都是特征标的整系数的线性组合：$\psi' - m\theta = \Sigma c_a \chi^a$，这给出

$$(\psi' - m\theta,\ \psi' - m\theta) = \Sigma c_a^2,$$

因而 $\Sigma c_a^2 = 1$，所以恰好存在一个 $c_a = \pm 1$ 而且其余的是零. 因此 $\psi' - m\theta = \pm\psi^a$. 然而 $(\psi' - m\theta)(1) = m > 0$，因而 $\psi' - m\theta = \psi^a$ 是 G 的特征标. 这证明了 $\psi' - m\theta$ 是特征标，因此 ω 是特征标，定理也就证明了.

16.9. 酉表示和正交表示

对于任意 $n \times n$ 矩阵 A：

$$A = (a_{ij}),\quad i, j = 1, \cdots, n, \tag{16.9.1}$$

可以对应一个双线性齐式 $B(y, x)$：

$$B(y, x) = \sum_{i,j} a_{ij} y_i x_j,\quad i, j = 1, \cdots, n, \tag{16.9.2}$$

而且反之，对于任意双线性齐式也可以对应一个矩阵 A. 我们关心的是双线性齐式中 y_i 和 x_i 的线性变换如何作用于对应的矩阵. 设

$$x_j = \sum_k c_{jk} x'_k,\quad j, k = 1, \cdots, n; \tag{16.9.3}$$

$$y_i = \sum_s d_{is} y'_s,\quad i, s = 1, \cdots, n.$$

那么

$$B(y, x) = B'(y', x') = \sum_{i,j,k,s} d_{is} a_{ij} c_{jk} y'_s x'_k. \tag{16.9.4}$$

因而 $B'(y', x')$ 对应于矩阵

$$A' = D^T A C,\ D = (d_{is}),\ C = (c_{jk}). \qquad (16.9.5)$$

我们不预备在这里讨论最广的双线性齐式，而只讨论某些特殊类型的双线性齐式．在整个这节中的系数都属于复数域．如果

$$a_{ji} = \bar{a}_{ij}, \quad i, j = 1, \cdots, n, \qquad (16.9.6)$$

这里 $\bar{a}_{ij}$ 表示 a_{ij} 的共轭复数，则就说矩阵 A 是埃尔米特矩阵．因而埃尔米特矩阵对应于埃尔米特齐式 $H(\bar{x}, x)$：

$$H(\bar{x}, x) = \sum_{i,j} a_{ij}\bar{x}_i x_j,\ a_{ji} = \bar{a}_{ij}, \quad i, j = 1, \cdots, n. \ (16.9.7)$$

注意在埃尔米特齐式或埃尔米特矩阵中，系数 $a_{ii} = \bar{a}_{ii}$ 是实数． 实埃尔米特矩阵是实对称矩阵，它对应于实二次齐式 $Q(x)$：

$$Q(x) = \sum_{i,j} a_{ij}x_i x_j,\ a_{ji} = a_{ij}, \quad i, j = 1, \cdots, n. \ (16.9.8)$$

保持埃尔米特齐式(或二次齐式)不变的非奇异线性变换显然组成一个群． 这时认为共轭数 $\bar{x}_i$ 经变换后变成的数共轭于 x_i 经变换后变成的数．

定义． 满足

$$\bar{U}^T I U = I \qquad (16.9.9)$$

的矩阵 U 叫做酉矩阵．

定义． 满足

$$V^T I V = I \qquad (16.9.10)$$

的矩阵 V 叫做正交矩阵．

酉矩阵和正交矩阵显然都是非奇异的，而且它们组成群．酉矩阵对应于保持 $\bar{x}_1 x_1 + \cdots + \bar{x}_n x_n$ 不变的线性变换，正交矩阵对应于保持 $x_1^2 + \cdots + x_n^2$ 不变的线性变换． 实数酉矩阵是正交矩阵，但是严格地说也存在不是实数的正交矩阵，例如

$$V=\begin{pmatrix} i, & \sqrt{2} \\ -\sqrt{2}, & i \end{pmatrix}. \tag{16.9.11}$$

不过在这里当我们说到正交矩阵时，指的总是实数矩阵.

如果矩阵 $\rho(g)$, $g\in G$ 都是酉矩阵，则群 G 的表示 $\rho(g)$ 叫做酉表示，又如果矩阵 $\rho(g)$, $g\in G$ 都是正交矩阵，则 $\rho(g)$ 叫做正交表示.

定理 16.9.1. 有限群 G 在复数(实数)域上的每个表示等价于一个酉(正交)表示.

证明: 如果在埃尔米特齐式

$$H(\bar{x},x)=\Sigma a_{ij}\bar{x}_i x_j,\quad a_{ji}=\bar{a}_{ij} \tag{16.9.12}$$

中，变数 x_i 给定复数值，则 H 是实数，因为我们可以把各项配对:

$$a_{ji}\bar{x}_j x_i+a_{ij}\bar{x}_i x_j=\bar{a}_{ij}\bar{x}_j x_i+a_{ij}\bar{x}_i x_j, \tag{16.9.13}$$

每一对都是一个复数和它的共轭复数的和. 对角项 $a_{ii}\bar{x}_i x_i$ 当然是实数. 如果 $H(\bar{x},x)$ 只在所有变数都取零值时才等于零，而在其他情形都是正数，则它叫做正定的. 明显地，正定性在变数经过非奇异线性变换时不变. n 个变数的一个特殊的正定齐式是

$$I(\bar{x},x)=\bar{x}_1x_1+\cdots+\bar{x}_nx_n, \tag{16.9.14}$$

这个齐式对应于单位矩阵. $I(\bar{x},x)$ 是正定的，因为除非 $x_j=0$ 对于 $j=1,\cdots,n$, 每一项 $\bar{x}_jx_j$ 都是正的.

引理 16.9.1. n 个变数的正定的埃尔米特齐式 $H(\bar{x},x)$ 可以变换成 $\bar{x}_1x_1+\cdots+\bar{x}_nx_n$.

我们注意到，对于正定的 $H(\bar{x},x)$:

$$H(\bar{x},x)=\sum_{i,j}a_{ij}\bar{x}_i x_j,\quad a_{ji}=\bar{a}_{ij},$$

每个对角系数 a_{rr} 都是正的. 因为否则，当 $a_{rr}\leqslant 0$, 令 $x_r=1$, $x_j=0$ 对于 $j\neq r$, 就有 $H(\bar{x},x)=a_{rr}\leqslant 0$ 而与正定性矛

盾．现在在

$$H' = \sum_{i,j} a_{ij}\bar{x}_i x_j, a_{ji} = \bar{a}_{ij},\ i,j = 1,\cdots,n \quad (16.9.15)$$

中，令

$$x_1' = \sqrt{a_{11}}\left(x_1 + \frac{a_{12}x_2}{a_{11}} + \cdots + \frac{a_{1n}x_n}{a_{11}}\right), \quad (16.9.16)$$

$$x_j' = x_j,\ j = 2,\cdots,n,$$

这是许可的变换，因为 a_{11} 是正的实数．我们容易算出

$$H = \bar{x}_1' x_1' + \Sigma b_{ij}\bar{x}_i' x_j',\quad i,j = 2,\cdots,n, \quad (16.9.17)$$

这里包含 $x_2',\cdots,x_n'$ 的项是这些变数的正定齐式，继续下去，我们最终把H变换成

$$H = \bar{x}_1 x_1 + \cdots + \bar{x}_n x_n. \qquad (16.9.18)$$

这就证明了引理．我们注意到，如果最初从H是实二次齐式Q开始，则同样的论证将把Q变换成 $x_1^2 + \cdots + x_n^2$．

现在设 $\rho(g),\ g\in G$ 是有限群G的 n 阶的复数表示，再设G的元素是 $g_1 = 1, g_2, \cdots, g_t$．那么

$$M = I + \overline{\rho(g_2)}^T I\rho(g_2) + \cdots + \overline{\rho(g_t)}^T I\rho(g_t) \quad (16.9.19)$$

是对应于一个正定埃尔米特齐式的矩阵，因为每一加项各别地对应于一个正定齐式．其次，对于任何 $g\in G$，

$$\overline{\rho(g)}^T M\rho(g) = \sum_{i=1}^{t} \overline{\rho(g)}^T\overline{\rho(g_i)}^T\rho(g_i)\rho(g)$$

$$= \sum_{i=1}^{t} \overline{\rho(g_i g)}^T\rho(g_i g)$$

$$= \sum_{i=1}^{t} \overline{\rho(g_i)}^T\rho(g_i) = M. \quad (16.9.20)$$

因此 M 所对应的正定埃尔米特齐式H在 $\rho(g),\ g\in G$ 下不变．如果当变数变换时：

$$x_j = \sum_{k=1}^{n} c_{jk}x_k',\quad j = 1,\cdots,n, \qquad (16.9.21)$$

H变换成 $\bar{x}'_1x'_1+\cdots+\bar{x}'_nx'_n=I(\bar{x}',x')$，则对应地，

$$\rho'(g)=C^{-1}\rho(g)C,\ C=(c_{jk}) \qquad (16.9.22)$$

是等价于 $\rho(g)$ 的酉表示，这就是我们要求证明的.

我们也可以以矩阵的方式来证明这一点. 我们有

$$\bar{C}^TMc=I,\ M=\bar{C}^{-1T}C^{-1}, \qquad (16.9.23)$$

而且对于每个 $g\in G$，

$$\overline{\rho(g)}^TM\rho(g)=M, \qquad (16.9.24)$$

或

$$\overline{\rho(g)}^T\overline{C^{-1}}^TC^{-1}\rho(g)=\overline{C^{-1}}^TC^{-1}, \qquad (16.9.25)$$

因而

$$\overline{(C^{-1}\rho(g)C)}^TC^{-1}\rho(g)C=I, \qquad (16.9.26)$$

所以 $\rho'(g)=C^{-1}\rho(g)C$ 是酉矩阵.

16.10. 群表示的几个例子

我们先提出物理学家关心的一个例子，把无限的矩阵群表示成另一个矩阵群. 二维的么模酉矩阵有形状

$$\begin{pmatrix}\alpha, & \beta\\ -\bar{\beta}, & \bar{\alpha}\end{pmatrix},\ \alpha\bar{\alpha}+\beta\bar{\beta}=1, \qquad (16.10.1)$$

这里 α 和 β 是满足条件 $\alpha\bar{\alpha}+\beta\bar{\beta}=1$ 的任意复数. 这种矩阵的群 U_2 是下列线性变换的群:

$$\begin{aligned}u&=\alpha u'+\beta v',\\ v&=-\beta u'+\alpha v',\end{aligned}\qquad \alpha\bar{\alpha}+\beta\bar{\beta}=1, \qquad (16.10.2)$$

它们保持 $\bar{u}u+\bar{v}v$ 不变. 我们可以用复变数 u 和 v 定义三个实变数

$$\begin{aligned}x_1&=\bar{u}v+\bar{v}u,\\ x_2&=\frac{1}{i}(\bar{u}v-\bar{v}u),\end{aligned} \qquad (16.10.3)$$

$$x_3 = \bar{u}u - \bar{v}v.$$

我们注意到

$$x_1^2 + x_2^2 + x_3^2 = (\bar{u}u + \bar{v}v)^2, \qquad (16.10.4)$$

把线性变换(16.10.2)代入(16.10.3)时导出 x_i 的实线性变换，它根据(16.10.4)属于实正交群 O_3. 由(16.10.2)导出的 x_i 的线性变换是

$$\begin{aligned}
x_1 = &\frac{1}{2}(\alpha^2 + \bar{\alpha}^2 - \beta^2 - \bar{\beta}^2)x_1' \\
&+ \frac{i}{2}(-\alpha^2 + \bar{\alpha}^2 - \beta^2 + \bar{\beta}^2)x_2' + (-\alpha\beta - \overline{\alpha\beta})x_3', \\
x_2 = &\frac{i}{2}(\alpha^2 - \bar{\alpha}^2 - \beta^2 + \bar{\beta}^2)x_1' \qquad (16.10.5) \\
&+ \frac{1}{2}(\alpha^2 + \bar{\alpha}^2 + \beta^2 + \bar{\beta}^2)x_2' + i(\overline{\alpha\beta} - \alpha\beta)x_3', \\
x_3 = &(\alpha\bar{\beta} + \beta\bar{\alpha})x_1' + i(\bar{\alpha}\beta - \beta\bar{\alpha})x_2' + (\alpha\bar{\alpha} - \beta\bar{\beta})x_3'.
\end{aligned}$$

因而群 U_2 在实三维正交群 O_3 中有由(16.10.5)给定的表示 ρ. 这个表示不是一一的，但是是二对一的，U_2 中的 $\begin{pmatrix}1, & 0\\0, & 1\end{pmatrix}$ 和 $\begin{pmatrix}-1, & 0\\0, & -1\end{pmatrix}$ 都由 O_3 的单位元素表示. U_2 由整个本义旋转(它们的行列式等于 $+1$)的群表示. 由本义旋转组成的任何群 G 在 U_2 内的逆象叫做**二重群** $2G$. 群 $2G$ 是属于它的中心的 2 阶子群借助于与 G 同构的商群的扩张.

保黎(Pauli[1])发现，如果物理体系 S 对应于群 O_3 的某个子群 K，则 S 的电子自旋的波函数对应于二重群 $2K$.

除(16.10.5)外，还有另一个公式给出 U_2 和它在 O_3 内的表示之间的明白的联系. 给了欧几里得三维空间的一个本义旋转(即 O_3 的一个元素)，设 OT 是坐标平面 XOY 与它的像 $X'OY'$ 的交线. 那么(参看图 7)如果 ϕ 是角 $X'OT$，ψ 是

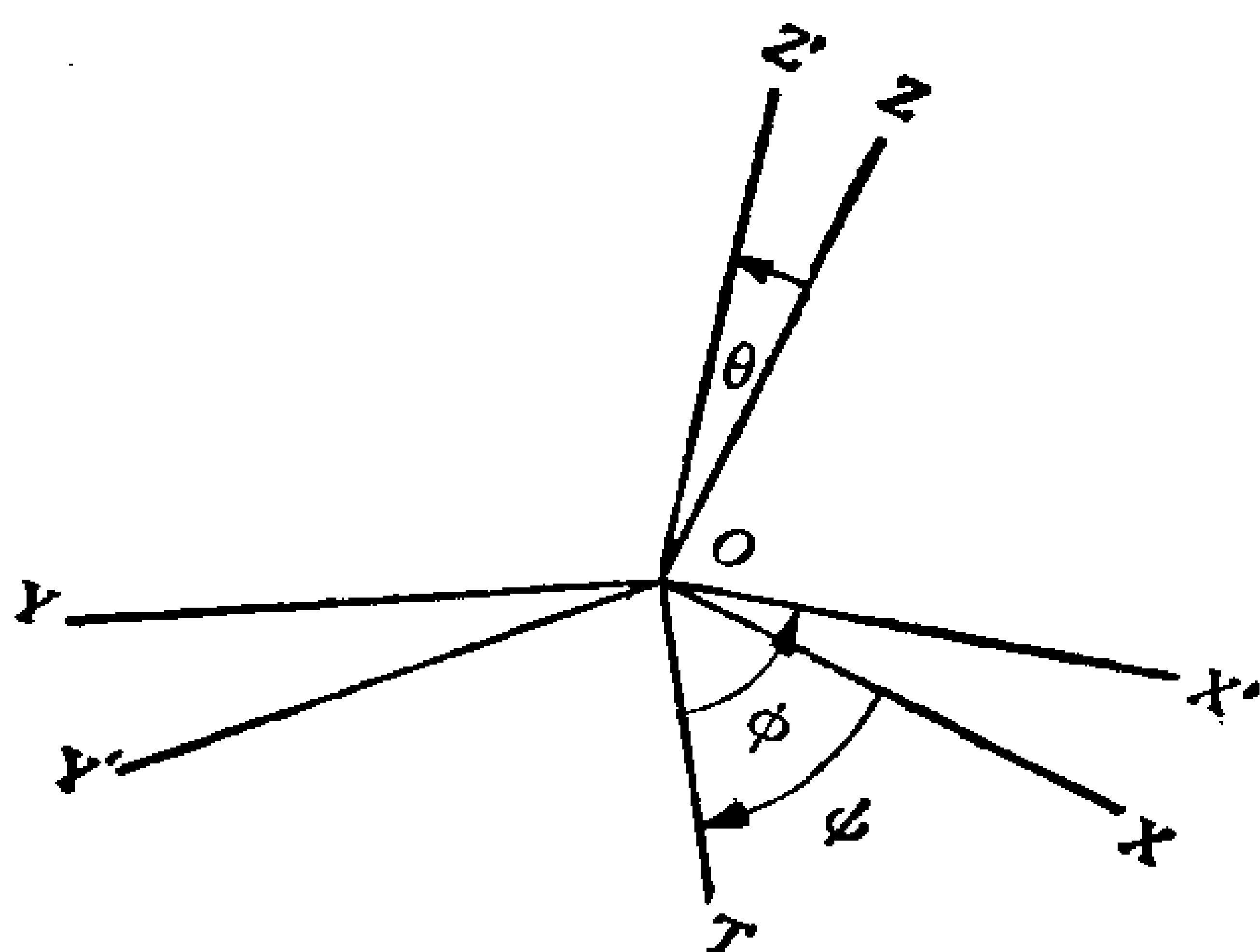


图7 三维旋转

角 XOT，θ 是角 ZOZ'，则可以在(16.10.1)中令

$$\alpha = \cos\frac{\theta}{2}\exp i\left(\frac{\phi+\psi}{2}\right),$$
$$\beta = i\sin\frac{\theta}{2}\exp i\left(\frac{\phi-\psi}{2}\right) \qquad (16.10.6)$$

而找出 U_2 的对应元素．当 XOY 和 $X'OY'$ 重合时(即对于绕 Z 轴的旋转)这也成立，这时只要令 $\theta=0$，$\phi=0$ 而且取 ψ 为绕 Z 轴的旋转角.

正四面体的本义旋转的群可以确切地表示成它的四个顶点的置换群．对于每个顶点，存在子群不变这个顶点而旋转对面的三个顶点，这是3阶群，不变两个顶点而交换另两个顶点的对称变换是对平面的反射，它改变定向，因而不是本义旋转．因此四面体的本义旋转的群是12阶的，而且它同构于四个文字的交替群 A_4．我们按共轭类列出元素：

$$\begin{aligned} C_1 &= (1),\\ C_2 &= (12)(34),\ (13)(24),\ (14)(23),\\ C_3 &= (123),\ (142),\ (134),\ (243),\\ C_4 &= (132),\ (124),\ (143),\ (234). \end{aligned} \qquad (16.10.7)$$

共轭类的乘法表是

$$
\begin{aligned}
C_1C_i &= C_iC_1 = C_i,\ i = 1, 2, 3, 4.\\
C_2^2 &= 3C_1 + 2C_2.\\
C_2C_3 &= C_3C_2 = 3C_3.\\
C_2C_4 &= C_4C_2 = 3C_4.\\
C_3^2 &= 4C_4.\\
C_3C_4 &= C_4C_3 = 4C_1 + 4C_2,\\
C_4^2 &= 4C_3.
\end{aligned}
\tag{16.10.8}
$$

我们现在在群环的中心 Z 内来找出组成 Z 的正交基底的幂等元素. 使 eZ 成为 Z 内的极小理想的幂等元素 e 是这种元素中的一个，反之亦然. 因此可以通过把 Z 分解成（双侧）理想的直和来找. 特别地说，任何零因子产生作为 Z 的真子集的理想. 因而通过寻求双侧理想中的零因子，我们可以找出较小的双侧理想，最终得出极小理想，于是可以由此得出正交的幂等元素. 一般地说，设 f 是 Z 内的幂等元素，如果 $fC_i = a_if$ 对于每个共轭类都成立，则 fZ 是 Z 内的极小理想，因而 f 是正交的幂等元素中的一个. 如果对于某个共轭类 C，fC 与 f 线性无关，则设 s 是最小整数，使得 fC^j, $j = 0, \cdots, s-1$ 线性无关，但是 fC^s 与它们线性相关. 于是我们有关系 $f(C^s + a_1C^{s-1} + \cdots + a_s) = 0$. 必要时把 $x^s + a_1x^{s-1} + \cdots + a_s = 0$ 的根添加到系数域. 如果 u 是这样的根，则 $f(C-u)$ 是理想 fZ 中的零因子，因而它导出较小的双侧理想. 这种一般的论证将在研究四面体群中使用.

对于任何 g 阶群 G，元素之和除以 g 得出一个幂等元素 e，它所对应的是 Z 的极小理想. 这个幂等元素对应于 G 的恒同表示. 现在这是 $e_1 = (C_1 + C_2 + C_3 + C_4)/12$. 我们还注意到，从 (16.10.8) 得出关系式

$$C_2^2 - 2C_2 - 3C_1 = (C_2 - 3C_1)(C_2 + C_1) = 0. \tag{16.10.9}$$

因而 $C_2 - 3C_1$ 和 $C_2 + C_1$ 都是零因子. 事实上我们发现

$(C_2-3C_1)Z$ 是极小理想而且 $e_2=(3C_1-C_2)/4$ 是生成这个极小理想的幂等元素。又 $e_1e_2=e_2e_1=0$。然后我们造出幂等元素 $f=1-e_1-e_2$，它必定是 Z 中剩下部分的单位元素。当然 fZ 必定是 2 维的而且 $f=e_3+e_4$，这里 e_3 和 e_4 是 Z 的一个正交基底中的另外两个幂等元素。这时我们发现

$$\begin{aligned}
f &= (2C_1+2C_2-C_3-C_4)/12,\\
fC_1 &= f,\\
fC_2 &= 3f,\\
fC_3 &= (-4C_1-4C_2+8C_3-4C_4)/12,\\
fC_4 &= (-4C_1-4C_2-4C_3+8C_4)/12.
\end{aligned} \tag{16.10.10}$$

理想 fZ 应该是 2 维的，而且我们注意到，线性相关式

$$fC_4+fC_3+4f=0 \tag{16.10.11}$$

成立，这说明 fZ 的维数确实是 2。我们还有下列关系。

$$f(C_3^2+4C_3+16)=0. \tag{16.10.12}$$

如果把复数立方单位根 $\omega=(-1+\sqrt{3}i)/2$ 添加到有理数域，则 (16.10.12) 可以改写成：

$$f(C_3-4\omega)(C_3-4\omega^2)=0. \tag{16.10.13}$$

因而由每个元素 $f(C_3-4\omega)$ 和 $f(C_3-4\omega^2)$ 生成的主理想都小于主理想 fZ。元素 $f(C_3-4\omega)$ 和 $f(C_3-4\omega^2)$ 分别与下面 (16.10.14) 中的幂等元素 e_3 和 e_4 相差一个纯量因子。

$$\begin{aligned}
e_1 &= (C_1+C_2+C_3+C_4)/12,\\
e_2 &= (3C_1-C_2)/4,\\
e_3 &= (C_1+C_2+\omega C_3+\omega^2C_4)/12,\\
e_4 &= (C_1+C_2+\omega^2C_3+\omega C_4)/12,\\
e_1 &+ e_2+e_3+e_4=C_1=1.
\end{aligned} \tag{16.10.14}$$

根据极小正交幂等元素以共轭类表出的式子，我们立即可以写出关于特征标的表，反之亦然。紧接着定理 16.6.10 之前，我们曾经建立一个关系式，它可以写成

$$C_k = h_k \sum_a \frac{\chi_k^a}{n_a} e_a. \qquad (16.10.15)$$

乘上 $\bar{\chi}_k^b$ 而且对 k 求和，我们得出

$$\sum_k \bar{\chi}_k^b C_k = \sum_{a,k} \frac{h_k \bar{\chi}_k^b \chi_k^a e_a}{n_a}. \qquad (16.10.16)$$

如果在上式右边先对 k 求和，而且利用正交关系

$$\sum_k h_k \bar{\chi}_k^b \chi_k^a = \delta_{ab} g, \qquad (16.10.17)$$

则当我们对 a 求和时，除 $a=b$ 外的各项都是零，因而(16.10.16)成为

$$\sum_k \bar{\chi}_k^b C_k = g e_b / n_b. \qquad (16.10.18)$$

我们把它改写成

$$e_b = \frac{n_b}{g} \sum_k \bar{\chi}_k^b C_k. \qquad (16.10.19)$$

因为单位元素的共轭类的特征标等于阶数：$\bar{\chi}_1^b = n_b$，所以关于 e_b 的(16.10.19)式中 C_1 的系数是 n_b^2/g。这决定了 n_b，然后我们可以利用(16.10.19)找出其余的特征标。

利用一般的公式(16.10.19)和关于四面体群的表(16.10.14)，我们可以写出关于它的特征标的表：

	C_1	C_2	C_3	C_4
ρ_1	1	1	1	1
ρ_2	3	-1	0	0
ρ_3	1	1	ω^2	ω
ρ_4	1	1	ω	ω^2

(16.10.20)

反之，根据关于特征标的表(16.10.20)，我们可以利用(16.10.19)写出(16.10.14)中的极小正交幂等元素。

三个一阶的不可约表示 ρ_1，ρ_3 和 ρ_4 可以直接根据关于特征标的表写出。

根据定理 16.6.15，把四面体群表成 A_4 的表示是恒同表示和一个不可约表示的和，这个不可约表示是 3 阶的，因而必定是 ρ_2. 变数 x_1, x_2, x_3 和 x_4 的属于 A_4 的置换不变线性齐式 $x_1+x_2+x_3+x_4$ 而且把由 $y_1=x_1-x_4$, $y_2=x_2-x_4=y_3=x_3-x_4$ 生成的补空间变成自己. 这时置换 (12) (34) 是线性变换

$$\begin{aligned} x_1 &= x_2', \\ x_2 &= x_1', \\ x_3 &= x_4', \\ x_4 &= x_3', \end{aligned} \tag{16.10.21}$$

而对于 y_i 这是

$$\begin{aligned} y_1 &= y_2' - y_3', \\ y_2 &= y_1' - y_3', \\ y_3 &= -y_3'. \end{aligned} \tag{16.10.22}$$

因此

$$\rho[(12)(34)] = \begin{pmatrix} 0, & 1, & -1 \\ 1, & 0, & -1 \\ 0, & 0, & -1 \end{pmatrix}. \tag{16.10.23}$$

同理

$$\rho[(123)] = \begin{pmatrix} 0, & 1, & 0 \\ 0, & 0, & 1 \\ 1, & 0, & 0 \end{pmatrix}. \tag{16.10.24}$$

因为元素 (12) (34) 和 (123) 生成整个群 A_4, 所以这个群的表示 ρ_2 完全确定了. 这不是 ρ_2 的正交形式，但是这可以从下一个例子得出，因为四面体群是八面体群的子群.

在第一章的例 2 中曾经讨论过立方体的对称变换的群. 立方体的本义旋转组成 24 阶群 G_{24}, 它由下列两个元素生成.

$$a=\begin{pmatrix}1,2,3,4,5,6,7,8\\2,3,4,1,6,7,8,5\end{pmatrix}=(1234)(5678)$$

和

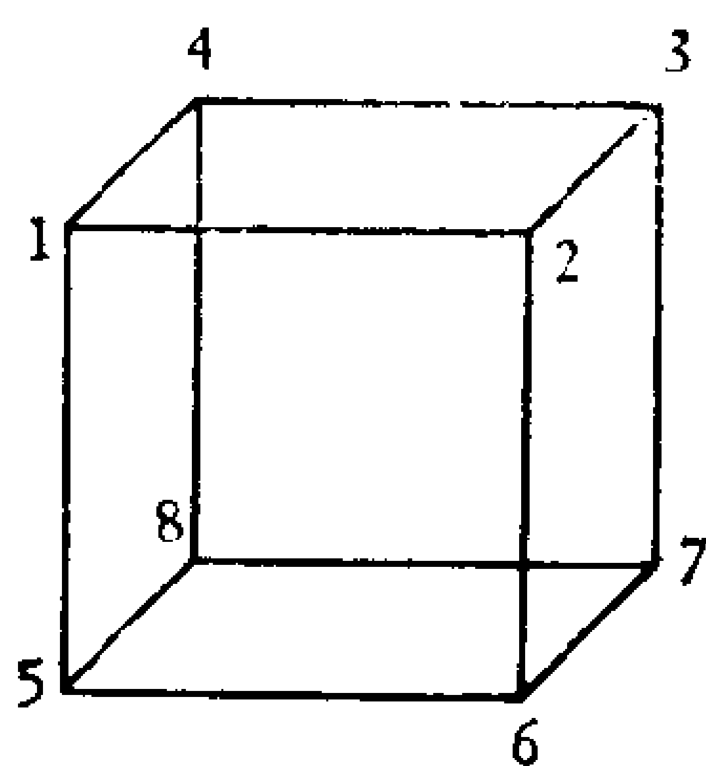


图 8　立方体的对称

$$b=\begin{pmatrix}1,2,3,4,5,6,7,8\\1,4,8,5,2,3,7,6\end{pmatrix}$$
$$=(1)(245)(7)(386).$$

群 G_{24} 也是正八面体的对称变换的群，可以取立方体各面中心作为顶点而得出内接于立方体的正八面体. 因此 G_{24} 可以表示成立方体的六个面(对应于内接八面体的六个顶点)上的置换群. 设八面体的六个顶点用三维坐标给出，我们用六个变数来表出这些顶点. 我们记:

变数	立方体的面	八面体的顶点
x_1	面 1234	(0,0,1)
x_2	面 1256	(0,1,0)
x_3	面 1458	(−1,0,0)
x_4	面 5678	(0,0,−1)
x_5	面 3478	(0,−1,0)
x_6	面 2367	(1,0,0)

于是 $a=(x_1)\ (x_4)\ (x_2,\ x_6,\ x_5,\ x_3)$, $b=(x_1,x_3,x_2)\ (x_4,x_6,x_5)$. G_{24} 的 24 个元素如下: 我们把每个元素既写成 x_i 上的置换，又写成产生八面体顶点的对应置换的坐标 x, y, z 的单项线性变换.

共轭类	g_i	置换	x,	y,	z
C_1	g_1	(x_1)	x,	y,	z
C_2	g_2	$(x_1)(x_4)(x_2,x_5)(x_3,x_6)$	$-x$,	$-y$,	z
	g_3	$(x_1,x_4)(x_2)(x_5)(x_3,x_6)$	$-x$,	y,	$-z$
	g_4	$(x_1,x_4)(x_2,x_5)(x_3)(x_6)$	x,	$-y$,	$-z$

	g_5	$(x_1)(x_4)(x_2,x_6,x_5,x_3)$	$-y$,	x,	z
	g_6	$(x_1)(x_4)(x_2,x_3,x_5,x_6)$	y,	$-x$,	z
	g_7	$(x_2)(x_5)(x_1,x_3,x_4,x_6)$	z,	y,	$-x$
C_3	g_8	$(x_2)(x_5)(x_1,x_6,x_4,x_3)$	$-z$,	y,	x
	g_9	$(x_3)(x_6)(x_1,x_2,x_4,x_5)$	x,	$-z$,	y
	g_{10}	$(x_3)(x_6)(x_1,x_5,x_4,x_2)$	x,	z,	$-y$
	g_{11}	$(x_1,x_2)(x_3,x_6)(x_4,x_5)$	$-x$,	z,	y
	g_{12}	$(x_1,x_3)(x_2,x_5)(x_4,x_6)$	$-z$,	$-y$,	$-x$
	g_{13}	$(x_1,x_4)(x_2,x_6)(x_3,x_5)$	y,	x,	$-z$
C_4	g_{14}	$(x_1,x_4)(x_2,x_3)(x_5,x_6)$	$-y$,	$-x$,	$-z$
	g_{15}	$(x_1,x_5)(x_2,x_4)(x_3,x_6)$	$-x$,	$-z$,	$-y$
	g_{16}	$(x_1,x_6)(x_2,x_5)(x_3,x_4)$	z,	$-y$,	x
	g_{17}	$(x_1,x_2,x_3)(x_4,x_5,x_6)$	$-z$,	$-x$,	y
	g_{18}	$(x_1,x_2,x_6)(x_3,x_4,x_5)$	z,	x,	y
	g_{19}	$(x_1,x_3,x_2)(x_4,x_6,x_5)$	$-y$,	z,	$-x$
C_5	g_{20}	$(x_1,x_3,x_5)(x_2,x_4,x_6)$	y,	$-z$,	$-x$
	g_{21}	$(x_1,x_5,x_3)(x_2,x_6,x_4)$	$-z$,	x,	$-y$
	g_{22}	$(x_1,x_5,x_6)(x_2,x_3,x_4)$	z,	$-x$,	$-y$
	g_{23}	$(x_1,x_6,x_2)(x_3,x_5,x_4)$	y,	z,	x
	g_{24}	$(x_1,x_6,x_5)(x_2,x_4,x_3)$	$-y$,	$-z$,	x

我们可以把 G_{24} 的这个表示中的偶置换（共轭类 C_1, C_2, C_5 中的置换）映成+1 而且把奇置换（共轭类 C_3, C_4 中的置换）映成−1. 这给出恒同表示以外的另一个一阶表示. 不可约表示的阶 n_i 满足关系

$$n_1^2 + n_2^2 + n_3^2 + n_4^2 + n_5^2 = 24. \qquad (16.10.25)$$

当 $n_1 = 1$, $n_2 = 1$ 时，我们得出 n_3, n_4, n_5 是 2, 3, 3. 上面表中给出的三阶表示有下列特征标:

$$\chi_1 = 3,\ \chi_2 = \chi(g_2) = -1,\ \chi_3 = \chi(g_5) = 1, \qquad (16.10.26)$$

$$\chi_4 = \chi(g_{11}) = -1, \ \chi_5 = \chi(g_{17}) = 0.$$

一般地说，如果

$$\rho = \sum_a c_a\rho_a \tag{16.10.27}$$

是表示 ρ 的展开成不可约表示 ρ_a 的和的式子，则对于第 i 个共轭类，我们有

$$\chi_i = \sum_a c_a\chi_i^a, \tag{16.10.28}$$

而且根据正交关系

$$\sum_i h_i\chi_i\bar{\chi}_i = g\sum_a c_a^2. \tag{16.10.29}$$

因为对于我们的 3 阶表示，从 (16.10.26) 得出

$$\sum_i h_i\chi_i\bar{\chi}_i = 24, \tag{16.10.30}$$

所以 $\sum_a c_a^2 = 1$，因而这个表示(我们把它记做 ρ_4) 是不可约的. 我们注意到 ρ_4 是正交的，而且因为偶置换 (共轭类 C_1, C_2, C_5 的元素)组成同构于四面体群的子群，所以我们得到 3 阶的正交表示，这是我们在讨论四面体群时所期望得出的.

现在我们有了关于特征标的一部分表：

	$h_1=1$	$h_2=3$	$h_3=6$	$h_4=6$	$h_5=8$
	C_1	C_2	C_3	C_4	C_5
ρ_1	1	1	1	1	1
ρ_2	1	1	-1	-1	1
ρ_3	2	y_2	y_3	y_4	y_5
ρ_4	3	-1	1	-1	0
ρ_5	3	z_2	z_3	z_4	z_5

(16.10.31)

从第二列对于第一列和对于它自己的正交条件，我们得出

$$1+1+2y_2-3+3z_2=0,$$
$$1+1+y_2^2+1+z_2^2=8. \tag{16.10.32}$$

这两个方程有解 $y_2=2$ 和 $z_2=-1$ 或 $y_2=-22/13$ 和 $z_2=19/13$. 因为 y_2 是 1 的两个平方根的和，所以 $y_2=\pm1\pm1$，因而第一组解 $y_2=2$ 和 $z_2=-1$ 是所要的值.

在第三列和前两列之间的正交关系给出

$$1-1+2y_3+3+3z_3=0,$$
$$1-1+2y_3-1-z_3=0. \tag{16.10.33}$$

因此 $y_3=0$ 和 $z_3=-1$. 用同样的方法可以找出其余各列的未知值. 总之，关于特征标的完全的表是：

(16.10.34)

	$h_1=1$	$h_2=3$	$h_3=6$	$h_4=6$	$h_5=8$
	C_1	C_2	C_3	C_4	C_5
ρ_1	1	1	1	1	1
ρ_2	1	1	−1	−1	1
ρ_3	2	2	0	0	−1
ρ_4	3	−1	1	−1	0
ρ_5	3	−1	−1	1	0

G_{24} 作为立方体顶点上的置换群的 8 阶表示 ρ 具有下列特征标：

(16.10.35)

	C_1	C_2	C_3	C_4	C_5
χ	8	0	0	0	2

从这些特征标可以找出 ρ 的分解式，因为如果

$$\rho=\sum_a c_a\rho_a, \tag{16.10.36}$$

$$\chi_i=\sum_a c_a\chi_i^a,$$

则根据正交性有

$$\sum_i h_i \chi_i \bar{\chi}_i^b = \sum_{i,a} c_a h_i \chi_i^a \bar{\chi}_i^b = g \sum_a c_a \delta_{ab} = g c_b. \quad (16.10.37)$$

这给出每个不可约表示 ρ_b 在 ρ 中出现的次数 c_b. 我们用这种方法从(16.10.35)得出

$$\rho = \rho_1 + \rho_2 + \rho_4 + \rho_5. \quad (16.10.38)$$

利用这个等式，可以从 ρ 求出 ρ_5. 利用(16.10.19)和关于特征标的表(16.10.34)，我们得出

$$e_5 = (3C_1 - C_2 - C_3 + C_4)/4. \quad (16.10.39)$$

G_{24} 的表示也是群环 R_G 的表示,因而我们得出 e_5 的表示是

$$\rho(e_5) = \frac{1}{4}\begin{bmatrix} 3, & -1, & -1, & -1, & -1, & -1, & 3, & -1 \\ -1, & -3, & -1, & -1, & -1, & -1, & -1, & 3 \\ -1, & -1, & 3, & -1, & 3, & -1, & -1, & -1 \\ -1, & -1, & -1, & 3, & -1, & 3 & -1, & -1 \\ -1, & -1, & 3, & -1, & 3, & -1, & -1, & -1 \\ -1, & -1, & -1, & 3, & -1, & 3, & -1, & -1 \\ 3, & -1, & -1, & -1, & -1, & -1, & 3, & -1 \\ -1, & 3, & -1, & -1, & -1, & -1, & -1, & 3 \end{bmatrix}.$$

(16.10.40)

取 $x_i = (0, \cdots, 1, \cdots, 0)$, $i = 1, \cdots, 8$ 作为 ρ 的表示模M的基底,那么矩阵 $\rho(e_5)$ 的各行生成子模 Me_5，它当然是 3 维的. 我们可以取前三行 r_1, r_2, r_3 作为基底. 但是更方便的是取与 $r_1 + r_3$, $r_1 + r_2$ 和 $r_2 + r_3$ 成比例的向量作为基底. 这个基底是

$$\begin{aligned} y_1 &= x_1 - x_2 + x_3 - x_4 + x_5 - x_6 + x_7 - x_8, \\ y_2 &= x_1 + x_2 - x_3 - x_4 - x_5 - x_6 + x_7 + x_8, \quad (16.10.41) \\ y_3 &= x_1 - x_2 - x_3 + x_4 - x_5 + x_6 + x_7 - x_8. \end{aligned}$$

在这个基底下我们有

$$\rho_5(a)=\begin{pmatrix}-1, & 0, & 0\\ 0, & 0, & -1\\ 0 & 1, & 0\end{pmatrix}=\begin{pmatrix}y_1, & y_2, & y_3\\ -y_1, & -y_2, & y_3\end{pmatrix}$$

(16.10.42)

$$\rho_5(b)=\begin{pmatrix}0, & 1, & 0\\ 0, & 0, & 1\\ 1, & 0, & 0\end{pmatrix}=\begin{pmatrix}y_1, & y_2, & y_3\\ y_2, & y_3, & y_1\end{pmatrix},$$

它们生成整个表示 ρ_5，因而 ρ_5 是 G_{24} 的由 (16.10.42) 给出的单项正交表示. 但是这不是本义旋转的群，因为我们看到 $\rho_5(a)$ 的行列式是 -1. 从 ρ_4 而且把对应于 C_3 和 C_4 的元素的矩阵乘上 -1 可以得到等价于 ρ_5 的表示，因此 ρ 等价于 ρ_4 和 ρ_2 的克朗耐克乘积.

表示 ρ_3 不是一一的，而具有由单位元素和 C_2 的元素组成的 4 阶核. 我们可以取下列生成元素

$$\rho_3(a)=\begin{pmatrix}0, & 1\\ 1, & 0\end{pmatrix},\quad \rho_3(b)=\begin{pmatrix}0, & 1\\ -1, & -1\end{pmatrix}. \tag{16.10.43}$$

在 G_{24} 作为本义旋转群的表示 ρ_4 中，我们有

$$\rho_4(a)=\begin{pmatrix}0, & -1, & 0\\ 1, & 0, & 0\\ 0, & 0, & 1\end{pmatrix},\quad \rho_4(b)=\begin{pmatrix}0, & -1, & 0\\ 0, & 0, & 1\\ -1, & 0, & 0\end{pmatrix}.$$

(16.10.44)

因而 ρ_4 是 O_3 的子群. 利用给出从 U_2 到 O_3 的映射的 (16.10.5) 式，我们得出

$$\begin{aligned}&\frac{\pm 1}{\sqrt{2}}\begin{pmatrix}1-i, & 0\\ 0, & 1+i\end{pmatrix}\to\rho_4(a),\\ &\frac{\pm 1}{2}\begin{pmatrix}1-i, & -1+i\\ 1+i, & 1+i\end{pmatrix}\to\rho_4(b).\end{aligned} \tag{16.10.45}$$

整个二重群 $D=2G_{24}$ 有八个共轭类. 一般地说，在二重群

2G 内，G 内的共轭类 C_i 的逆象或者是 2G 的共轭类但是元素个数两倍于 G 的共轭类 C_i，或者是两个共轭类 C'_i 和 $C''_i = -C'_i$，每个共轭类的元素个数都与 G 的共轭类 C_i 相同.

按照贝特（Bethe[1]）所说，我们可以用下列四个矩阵表出 D 的元素：

$$1 = \begin{pmatrix}1, & 0\\0, & 1\end{pmatrix}, \quad \sigma_x = \begin{pmatrix}0, & 1\\1, & 0\end{pmatrix},$$
$$\sigma_y = \begin{pmatrix}0, & -i\\i, & 0\end{pmatrix}, \quad \sigma_z = \begin{pmatrix}1, & 0\\0, & -1\end{pmatrix}. \tag{16.10.46}$$

按共轭类列出的 D 的元素是：

$$E = [1],$$
$$R = [-1],$$
$$C_2 = \pm[-i\sigma_x, -i\sigma_y, -i\sigma_z],$$
$$C'_3 = \left[\frac{1 \pm i\sigma_x}{\sqrt{2}}, \frac{1 \pm i\sigma_y}{\sqrt{2}}, \frac{1 \pm i\sigma_z}{\sqrt{2}}\right], \tag{16.10.47}$$
$$C''_3 = -C'_3,$$
$$C_4 = \pm\left[\frac{-i(\sigma_y \pm \sigma_z)}{\sqrt{2}}, \frac{-i(\sigma_z \pm \sigma_x)}{\sqrt{2}}, \frac{-i(\sigma_x \pm \sigma_y)}{\sqrt{2}}\right],$$
$$C'_5 = \Big[\frac{1}{2}\{1 \pm i(\sigma_x + \sigma_y + \sigma_z)\},$$
$$\frac{1}{2}\{1 \pm i(-\sigma_x + \sigma_y - \sigma_z)\},$$
$$\frac{1}{2}\{1 \pm i(-\sigma_x - \sigma_y + \sigma_z)\},$$
$$\frac{1}{2}\{1 \pm i(\sigma_x - \sigma_y - \sigma_z)\}\Big],$$
$$C''_5 = -C'_5.$$

因为 G_{24} 是 D 的同态像，G_{24} 的每个不可约表示也是 D 的不可约表示. 而 D 还有其他的三个不可约表示，它们事实上

是D的一一表示．这些表示的特征标是：

	E	R	C_2	C_3'	C_3''	C_4	C_5'	C_5''
ρ_6	2	-2	0	$\sqrt{2}$	$-\sqrt{2}$	0	1	-1
ρ_7	2	-2	0	$-\sqrt{2}$	$\sqrt{2}$	0	1	-1
ρ_8	4	-4	0	0	0	0	-1	1

(16.10.48)

第十七章　自由乘积和共合乘积

17.1. 自由乘积的定义

设 G_i 是具有指标 $i \in I$ 的群组，这里假定 I 是有序的. 我们将用类似于定义具有已知生成者的方式来定义群 G_i 的自由乘积 $\prod_i^* G_i$

考虑字（或串）

$$a_1a_2\cdots a_t, \tag{17.1.1}$$

它们或是空的（记做 1），或者每个 a_i, $i = 1, \cdots, t$ 是某个 G_i 的元素. 对于这种字我们定义初等等价:

$(E1)$ $a_1a_2\cdots a_{i-1}a_ia_{i+1}\cdots a_t$ 等价于 $a_1\cdots a_{i-1}a_{i+1}\cdots a_t$, 假如 a_i 是某个群 G_j 的单位元素.

$(E2)$ $a_1a_2\cdots a_{i-1}a_ia_{i+1}\cdots a_t$ 等价于 $a_1a_2\cdots a_{i-1}a_i^*a_{i+2}\cdots a_t$, 假如 a_i 和 a_{i+1} 属于同一个群 G_j 而且在 G_j 内 $a_ia_{i+1} = a_i^*$.

我们自然认为初等等价是对称的. 我们说两个字 x 和 y 是等价的，假如存在有限序列 $x_1 = x$, x_2, x_3, $\cdots$, $x_n = y$, 使得 x_i 和 x_{i+1} 对于 $i = 1, 2, \cdots, n-1$ 都是初等等价的. 所有等价的字组成一类.

字 $a_1a_2\cdots a_t$ 叫做简化的，假如它是空的，或者假如 (1) 没有 a_i 是它所属的群 G_j 的单位元素而且 (2) a_i 和 a_{i+1} 对于 $i = 1, \cdots, t-1$ 总属于不同的群. 像在 § 7.1 中一样我们可以定义字 $f = a_1a_2\cdots a_t$ 的W过程，令:

$W_0 = 1$.

$W_1 = 1$，当 a_1 是它所属的群的单位元素时.

$W_1 = a_1$，其他情形，

当 W_i 具有简化形式 $b_1b_2\cdots b_s$ 时，令

1) $W_{i+1} = b_1\cdots b_s a_{i+1}$，假如 a_{i+1} 不是它所属的群的单位元素而且与 b_s 不属于同一个群.

2) $W_{i+1} = b_1\cdots b_s$，假如 a_{i+1} 是它所属的群的单位元素.

3) 如果 b_s 和 a_{i+1} 属于同一个群而且 $b_s a_{i+1} = 1$，则令 $W_{i+1} = b_1\cdots b_{s-1}$.

4) 如果 b_s 和 a_{i+1} 属于同一个群而且 $b_s a_{i+1} = b_s^* \neq 1$，则令 $W_{i+1} = b_1\cdots b_{s-1}b_s^*$.

于是像在 § 7.1 中一样，可以证明 $W(f) = W_t$ 是简化的，而且可以证明，对于初等等价的字，W 过程给出同样的结果，因而对于整个等价字类都是如此. 因此在每一类中存在唯一的简化字. 如果 $f = a_1\cdots a_t$ 是简化的，则 t 叫做 f 的**长度**.

我们可以定义字类的乘积，令

$$[f_1][f_2] = [f_1f_2], \tag{17.1.2}$$

按照定理 7.1.1 的证明，我们可以证明这个乘积不依赖于代表的选取. 这个乘法是可结合的而且组成以空字作为单位元素的群，这个群叫做群 G_i 的自由乘积 $\overset{*}{\prod\limits_i} G_i$. 根据 $(E1)$，我们看到每个群 G_i 的单位元素都等价于空字 1. 我们以后可以不区别这些单位元素. 不同的群的 $\neq 1$ 的元素是不同的简化字，因而是不同的.

定理 17.1.1. 设群 G 是子群 H_i，$i \in I$ 的并，这里 H_i 与群 G_i 同构. 那么 G 是自由乘积 $Q = \overset{*}{\prod\limits_i} G_i$ 的同态像.

证明. 像在定理 7.1.2 中一样，考虑 Q 的元素 $a_1a_2\cdots a_t$.

如果 a_i 是 G_j 的元素，则用 b_1 表示 H_j 的对应元素而建立到上的对应 $a_1a_2\cdots a_t\to b_1b_2\cdots b_t$. 于是 Q 的等价的字映成 G 的同一个元素. 从 Q 到 G 上的这个映射保持乘积，因而它是从 Q 到 H_j 的并 G 上的同态.

17.2. 共合乘积

设 G_i, $i\in I$ 是以 I 为指标集的群组. 设每个 G_i 包含一个子群 U_i，而且所有 U_i 都同构于已知群 U. 必须强调的是，在每个 U_i 和 U 之间存在着已知的特殊同构. 我们希望讨论由 G_i 生成的最一般的群，在其中所有 U_i 彼此等同起来，因而成为同构于 U 的同一个群 U^1. 明白地，这是 G_i 的自由乘积的这样的同态像：如果在 U_i, U_j 和 U 之间的已知同构下，$u_i\in U_i$ 和 $u_j\in U_j$ 对应于同一个元素 $u\in U$，则把 u_i 和 u_j 等同起来. 固然这种群一定存在，但是完全不清楚在这些基本的等同的基础上将会引起自由乘积中的怎样的等同. 特别地，也可能出现使所有元素都与单位元素等同的结果. 这种情形不会出现，因为这种等同实质上只作用于 U_i 的元素.

我们来造出由具有彼此等同的子群 U_i 的群 G 所生成的群，我们把它叫做 G_i 的**共合乘积**. 考虑字 $a_1a_2\cdots a_t$，这里每个 a_i 属于某个 G_j. 我们定义初等等价:

(*E*1) **如果** $a_i=1$，**则**

$$a_1a_2\cdots a_{i-1}a_ia_{i+1}\cdots a_t$$

等价于 $a_1a_2\cdots a_{i-1}a_{i+1}\cdots a_t$.

(*E*2) **如果** a_i 和 a_{i+1} **属于同一个群** G_j **而且在** G_j **内有** $a_ia_{i+1}=a_i^*$，**则**

$$a_1a_2\cdots a_ia_{i+1}\cdots a_t.$$

等价于 $a_1a_2\cdots a_i^*\cdots a_t$.

(E3) 如果 $a_i = u_i$ 是 $U_i \subseteq G_i$ 的元素而且 $b_i = u_k \in U_k$ 是这样的元素，使得在 U_i，U_k 和 U 的同构下，u_i 和 u_k 对应于同一个元素 $u \in U$，则

$$a_1 \cdots a_{i-1} a_i a_{i+1} \cdots a_t$$

等价于 $a_1 \cdots a_{i-1} b_i a_{i+1} \cdots a_t$.

我们现在说字 x 和 y 是等价的，假如存在有限序列 $x = x_1, x_2, \cdots, x_n = y$，使得 x_i 和 x_{i+1} 对于 $i = 1, \cdots, n-1$ 都是初等等价的. 等价字类成为一个群的元素，只要定义 $[f]$ 和 $[g]$ 的乘积为 $[fg]$. 像在定理 7.1.1 中一样，这个乘积对于等价字类有意义，而且对于这个乘积而说，这些类组成群 T，它是具有共合子群 U 的 G_i 的自由乘积. 以后把 T 简单叫做 G_i 的共合乘积. 但是我们还不知道 T 的本质. 为此需要提出 T 的元素的标准形式.

我们将定义对应于字 $f = a_1 a_2 \cdots a_t$，$a_i \in G_i$ 的标准形式. 然后必须证明这个标准形式对于等价的字是相同的，于是就证明了它是 T 的元素的标准形式.

对于每个 G_i，$i \in I$，设 x_{ik} 是 U_i 的左傍系的代表，这时取 G_i 的单位元素作为 U_i 的代表，其余的代表是任意选取的.

$$G_i = U_i + U_i x_{i2} + \cdots + U_i x_{in_i}, \quad i \in I. \qquad (17.2.1)$$

根据初等等价 (E1)，空字是 T 的单位元素也是所有 G_i 的单位元素. 又根据 (E3)，我们可以认为所有 U_i，$i \in I$ 都与 U 等同. 于是可以把 (17.2.1) 改写成

$$G_i = U + U x_{ix} + \cdots + U x_{in_i}, \quad i \in I. \qquad (17.2.2)$$

因此元素 $g_i \in G_i$ 可以记做

$$g_i = u \text{ 或 } g_i = uz, \; u \in U, \; z = x_{ik} \neq 1. \qquad (17.2.3)$$

在共合乘积中适宜于把字的长度的通常定义改变一下. 我们定义 $l(a_0 a_1 \cdots a_t) = t$ 如果 $a_0 \in U$，又 $l(a_1 \cdots a_t) = t$ 如果 $a_1 \notin U$. 因而当第一个字母是 U 的元素时我们不计这个字母.

我们说字 f 具有标准形式，假如

$$f = uz_1z_2\cdots z_t, \tag{17.2.4}$$

这里 $u\in U, z_j, j=1,\cdots,t$ 是(17.2.2)中的傍系代表 $x_{ik}\neq 1$，而且 z_j 和 z_{j+1} 对于 $j=1,\cdots,t-1$ 属于不同的 G_i.

定理 17.2.1. 在具有共合子群 U 的群 G_i 的共合乘积中，在每个等价字类内存在唯一的一个标准形式的字 $f=uz_1z_2\cdots z_t$. 这里 $u\in U$, z_i, $i=1,\cdots,t$ 是在 G_j 中任意取定的 U 的傍系代表 $x_{ik}\neq 1$，而且 z_i 和 z_{i+1}, $i=1,\cdots,t-1$ 属于不同的 G_i.

这个定理的证明很像 § 7.1 中的引理的证明. 为了简省篇幅我们略去了细节. 关于这方面的更进一步的探讨可以参看诺伊曼的论文 (H. Neumann [1, 2]).

17.3. 库罗什定理

库罗什[1]证明了自由乘积的每个子群本身是自由乘积. 这个结论将在下面证明. 具有共合子群的自由乘积的子群本身不一定是这种类型的. 如果 U 是共合子群，则当在自由乘积中存在两个以上的群 G_i 时，我们可以在 G_i 中取与 U 有不同交集的子群 H_i. 于是不同的 H_i 将以不同的方式等同起来，因而我们接触到所谓广义的共合乘积. 这时产生了一系列的复杂性. 这个理论直到现在还不完备.

定理 17.3.1 (库洛什定理). 自由乘积

$$G=\prod_v^* A_v$$

1) 参看 A. Kurosch (Курош) [1]. 下面的证明是由作者 (M. Hall [7]) 提出的.

的子群 $H \neq 1$ 本身是自由乘积：

$$H = F * \prod_j^* x_j^{-1} U_j x_j,$$

这里 F 是自由群而且每个 $x_j^{-1} U_j x_j$ 是 G 的某个自由因子 A_ν 的子群的共轭子群.

证明. G 的所有自由因子的元素可以排成良序：先是单位元素，然后取自由因子的一个顺序，而且在每个自由因子内取 $\neq 1$ 的元素的一个顺序. 在这个顺序的基础上来定义 G 的元素的字典顺序. 写下 G 的元素 g 的简化形式:

$$g = a_1 a_2 \cdots a_t.$$

空的乘积是单位元素；而对于 $g \neq 1$，每个 a_i 是某个自由因子 A_ν 的 $\neq 1$ 的元素，而且没有相继的两项 a_i, a_{i+1} $(i = 1, \cdots, t-1)$ 属于同一个自由因子 A_ν. 元素 g 的长度 $l(g)$ 定义为：当 $g = 1$ 时是零，而当 $g \neq 1$ 时是它的简化形式中的字母数 t. 我们用下列方法定义元素的字典顺序[1]:

1) 较短的字在较长的字之前.

2) 长度相等的字比较字母. 在第一个字母不同时按第一个字母的顺序来定字的顺序，在第一个字母相同而第二个字母不同时按第二个字母的顺序来定字的顺序，依此下去.

这显然是 G 的元素的一个良序.

现在来定义 G 的元素的第二个顺序——半字典顺序. 为此我们把偶数长度 $t = 2r$ 的元素 g 记做 $g = \alpha\beta^{-1}$，这里 $l(\alpha) = l(\beta) = r$，而且把奇数长度 $t = 2s + 1$ 的元素 g 记做 $g = \alpha a_{s+1}\beta^{-1}$，这里 $l(\alpha) = l(\beta) = s$. 元素 g 的半字典顺序是这样定义的[2]:

1) 先比较 g 的长度；

---

1), 2) 这里的定义参照俄译本改写. ——译者

2）对于具有相等的偶数长度的元素 $g=\alpha\beta^{-1}$，比较字 α 的字典顺序，在 α 相同时比较字 β 的字典顺序.

3）对于具有相等的奇数长度的元素 $g=\alpha a_{s+1}\beta^{-1}$，像上面一样，先比较 α 的字典顺序，后比较 β 的字典顺序，而在 α 和 β 都相同时则比较 a_{s+1} 的字典顺序.

G 的子群 H 是自由乘积的证明将要这样进行，使用半字典顺序来选取 H 的一个子集 K，而且证明：（1）K 的元素生成 H，然后是（2）K 的元素生成自由乘积

$$F^* \prod_j^* x_j^{-1}U_jx_j, \tag{17.3.1}$$

这里 F 是自由群而且每个 U_j 是某个自由因子 A_ν 的子群.

集合 K 由所有这样的元素 $k\neq 1$ 组成：（1）$k\in H$，而且（2）k 不属于由 H 中按半字典顺序说在 k 之前的元素生成的群.

因为 $H\neq 1$，H 中的第一个 $k\neq 1$ 属于集合 K，所以 K 不是空的. 考虑由集合 K 生成的群 $|K|$. 显然 $|K|\subseteq H$. 如果 $|K|\neq H$，则必定存在第一个 $h\in H$ 使得 $k\notin |K|$. 这种 h 不属于 H，因而它是 H 中在 h 之前的某些元素 h_i 的乘积. 但是这些 h_i 属于 $|K|$，因而作为这些 h_i 的乘积的 h 也属于 $|K|$. 因此 $|K|=H$，这完成了证明的第一部分.

我们将使用数值不等号 $<$ 同时表示字典顺序和半字典顺序. 从文中可以清楚理解它的意义：半字典顺序用于整个的字，而字典顺序则用于字的前半或后半. 把 $u\neq 1$ 记做 $u=\alpha\beta^{-1}$ 或 $u=\alpha a\beta^{-1}$. 对于偶数长度的字不会有 $\beta=\alpha$，因为 $\alpha\alpha^{-1}=1$. 对于奇数长度的字，$\beta=\alpha$ 是可能的；当 α 是固定的字，而且 a 属于某个固定的 A_ν 时，H 中形状为 $\alpha a\alpha^{-1}$ 的元素与单位元素共同组成子群 $\alpha B\alpha^{-1}$，它共轭于 $B\subseteq A_\nu$. 我们把元素 $\alpha a\alpha^{-1}$ 叫做**变形**. 我们把集合 K 扩大成较大的集合 T，

除K的元素外，对于每个α和A_v，T还包含由属于K的变形$\alpha a\alpha^{-1}(a\in A_v)$生成的变形$\alpha a^1\alpha^{-1}(a^1\in A_v)$，因此$T$由$H$中这样的元素组成：它不被在它之前的元素和由同一类型在前的变形生成的变形$\alpha a\alpha^{-1}$等生成.

元素$h\in H$可以写成

$$h=u_1u_2\cdots u_t, \tag{17.3.2}$$

这里$u_i\in T$或T^{-1}（由T中的元素的逆组成）. 其次，可以取(17.3.2)使得(a) $u_iu_{i+1}\neq 1$ $(i=1,\cdots,t-1)$和(b)任何两个相继的u_i和u_{i+1}都不属于同一个共轭群$\alpha B\alpha^{-1}$, $B\subseteq A_v$. 如果这两个条件满足，则说$u_1\cdots u_t$是半简化的.

要是能证明任何非空的半简化的字不可能是单位元素，定理就能立刻得出. 因为由此得出K中不是变形的元素生成自由群F，而且H是F和共轭群$\alpha B\alpha^{-1}$, $B\subseteq A_v$的自由乘积.

如果u是K的元素，而且$u^{-1}\neq u$，则$u<u^{-1}$，因为$u=(u^{-1})^{-1}$而且u^{-1}不能在u之前. 又如果$u\neq v$是K的元素，则$w=u^\varepsilon v^\eta$ $(\varepsilon,\eta=\pm 1)$将在u和v之后，因为u, v, w中的任何两个生成第三个，而且根据K的取法u和v都不能被在前的元素生成. 这两个结果是研究集合T和T^{-1}的元素相乘的基础. 在简化G中的乘积$a_1a_2\cdots a_m$时，这里每个a_i属于某个自由因子，如果a_i和a_{i+1}属于同一个自由因子A_v而且$a_ia_{i+1}=a_i'\neq 1$，则说a_i和a_{i+1}合并成a_i'，又如果$a_ia_{i+1}=1$，则说它们消去了.

引理 17.3.1. 如果$u=\alpha\beta^{-1}$或$\alpha a\beta^{-1}\in T$而且$\beta\neq\alpha$，则$\alpha<\beta$.

证明. 因为$\beta\neq\alpha$，我们有$u\in K$，又如果$\beta<\alpha$，则$u^{-1}<u$. 因而T的元素有三种：

1) $l(u)$是偶数，$u=\alpha\beta^{-1}$, $\alpha<\beta$, $u\in K$.

2) $l(u)$是奇数，$u=\alpha a\beta^{-1}$, $\alpha<\beta$, $u\in K$.

3）$l(u)$是奇数，$u=\alpha a\alpha^{-1}$，它由K中同类的变形生成。

引理 17.3.2. 如果$u \neq v$属于T而且不属于同一个共轭群$\alpha B\alpha^{-1}$，又w是$u^{\varepsilon}v^{\eta}$或$v^{\eta}u^{\varepsilon}$（$\varepsilon, \eta=\pm 1$）中的一个，则w在半字典顺序中在u和v之后。这导出在乘积w中作消去或合并的下列限制：

1）如果$u=\alpha\beta^{-1}$，则β不消去，又如果α消去，则β^{-1}的邻接的字母不合并。

2）如果$u=\alpha a\beta^{-1}$，$\alpha<\beta$，则α和a不消去，又如果β消去，则a不合并。

3）如果$u=\alpha a\alpha^{-1}\in\alpha B\alpha^{-1}$，则$\alpha$和$a$不消去，又如果$v^{\eta}=\alpha a^{1}\sigma$，这里$a$，$a^{1}\in A_{v}$，则$a^{1}$是傍系$Ba^{1}$的最前的元素。

证明. 在属于T的两个不同元素u和v中，设u是较前的，即$u<v$，如果w不在u和v之后，则$w<v$。这时不会出现$w=v$的情形。因为这将导出$u=1$（这不可能成立），或者$u=v^{2}$或v^{-2}。然而变形v的平方是1或同类的变形，而如果v不是变形，则$l(v^{2})>l(v)$。在这两种情况下，$u=v^{2}$或v^{-2}都是不可能的。

因为u，v，w中的任何两个生成第三个，所以当v属于K时，w必定是最后一个。因此我们只需要考虑$v=\alpha a\alpha^{-1}\in\alpha B\alpha^{-1}$是变形的情形。因为$u<v$而且$u\notin\alpha B\alpha^{-1}$，所以$u<v^{*}$，这里$v^{*}$是$\alpha B\alpha^{-1}$中的任何变形。因此，如果在$u$和$v$之间的消去只牵涉到$\alpha$（或$\alpha^{-1}$），则在$u$和某个$v^{*}=\alpha a^{*}\alpha^{-1}\in K$之间也将如此，这将产生乘积$w^{*}=u^{\varepsilon}v^{*}$或$v^{*}u^{\varepsilon}$，这里$w^{*}<v^{*}$，而与$v^{*}\in K$矛盾。因此，在$u$和$v$之间不仅消去$\alpha$，而且要消去或合并中心项$a$。总之$u^{\varepsilon}=\alpha a''\sigma^{-1}$，这里$a''$与$a$合并或消去。因为$u<v=\alpha a\alpha^{-1}$，所以或者$l(\sigma)<l(\alpha)$，或者$l(\sigma)=l(\alpha)$而且$u=\sigma a''^{-1}\alpha^{-1}$，这里$\sigma<\alpha$。在每一种情况下都有$u$和$\sigma(a''^{-1}a^{*}a'')\sigma^{-1}$生成$v^{*}=\alpha a^{*}\alpha^{-1}\in K$

而且在它之前，这是一个矛盾．总之当 $w<v$ 时在所有的情况下都导出矛盾，因而 w 在 u 和 v 之后．

由于所有八个乘积 $u^{\varepsilon}v^{\eta}$ 和 $v^{\eta}u^{\varepsilon}$ 都在 u 和 v 之后，所以有列举在定理中的关于消去和合并的限制．这些限制明白地说就是：不论是 u 或 v 都不能消去一半以上，而且在把一个元素的首段（或末段）与另一个元素的同样长度的一段进行消去和合并时，结果得到在顺序上较后的元素．

引理 17.3.3. 对于乘积 $u_1u_2\cdots u_t$，这里 $u_i\in T\cup T^{-1}(i=1,\cdots,t)$，$u_iu_{i+1}\neq 1\ (i=1,\cdots,t-1)$，而且 u_i 和 u_{i+1} 不属于同一个群 $\alpha B\alpha^{-1}(B\subseteq A_\nu)$，简化形式的末尾如下：

1）β^{-1}，如果 $u_t=\alpha\beta^{-1}$.

2）$b^*\alpha^{-1}$，如果 $u_t=(\alpha\beta^{-1})^{-1}$.

3）$a^*\beta^{-1}$，如果 $u_t=\alpha a\beta^{-1}$，$\alpha<\beta$.

4）$a^{-1}\alpha^{-1}$，如果 $u_t=(\alpha a\beta^{-1})^{-1}$，$\alpha<\beta$.

5）$a^*\alpha^{-1}$，如果 $u_t=\alpha a\alpha^{-1}$.

这里（2）中的 b^* 和（5）中的 a^* 或者是 u_t 中紧接在 α^{-1} 之前的字母，或者是它与 u_{t-1} 中的同类项合并的结果．在（3）中，a^* 可以包括与 u_{t-1} 和 u_{t-2} 的合并．

证明．这个引理可以用对 t 施行归纳法来证明，当 $t=1$ 时引理显然成立．当 $t=2$ 时，直接从引理 17.3.2，而且考虑到对于 $u=\alpha\beta^{-1}$ 或 $\alpha a\beta^{-1}$，在 u^2 中作消去时不会完全消去 α 和 β，就能得出结果．在证明从 t 到 $t+1$ 的归纳步骤时，我们只需要把引理 17.3.2 应用到上列各种情形里，而且还应用到 u_{t+1} 的五种可能情形里，这时还要用到从引理 17.3.2 不能立即得出的一个外加的性质．这性质是这样的：可能发生 $u_t=\alpha a\alpha^{-1}$，使得消去 α 和合并 a 能够同时对 $u_{t-1}=\sigma a'^{-1}\alpha^{-1}$ 和 $u_{t+1}=\alpha a''\lambda$ 进行．于是根据引理 17.3.2，a' 和 a'' 都是它们的傍系 Ba' 和 Ba'' 中的最先的元素．如果 $a'^{-1}aa''=1$，则

a'和a''属于同一个傍系，因而$a' = a''$，$a = 1$，$u_t = 1$，这是一个矛盾．因此$a'^{-1}aa'' \neq 1$，而且$u_{t-1}u_tu_{t+1}$的简化形式是$\sigma(a'^{-1}aa'')\lambda$．这是在半简化形式的乘积$u_1u_2\cdots u_m$中可以把多到相继的三项作合并的唯一方式．

在确定了半简化形式$h = u_1u_2\cdots u_t$的简化形式的结尾以后，我们当然也就证明$h \neq 1$，因而H是由元素$\alpha\beta^{-1}$和$\alpha a^{-1}\beta^{-1}(\alpha < \beta)$生成的无限循环群和自由因子$A_\nu$的子群$B$的共轭群$\alpha B\alpha^{-1}$的自由乘积．

第十八章　伯恩赛德问题

18.1. 问题的表述

在 1902 年伯恩赛德（Burnside [1]）写了"离散群理论的一个未解决的问题：是否可以有无限阶群，它的元素都是有限阶的". 他讨论的是有限生成群. 这个问题还没有解决[1]. 一般意义下的这个问题并未真正被讨论过. 他讨论了这个问题的较特殊的形式：假定已知群是有限生成的而且它的元素的阶是有界的.

如果 G 由 r 个元素生成而且 n 是 G 的元素的阶的最小公倍数，则问题是：G 是有限群吗？这个问题是熟知的伯恩赛德问题. 如果 $x_1, \cdots, x_r$ 生成群 $B(n, r)$，而且对于每个 $g \in B(n, r)$ 都有关系 $g^n = 1$，则这个群叫做由 r 个元素生成的 n 阶伯恩赛德群[2]. 明显地，具有 r 个生成元素而且元素的阶整除 n 的每个群都是这个特殊的群的同态像. 于是伯恩赛德问题成为这样：群 $B(n, r)$ 中那些是有限群？

如果 F_r 是由 $x_1, \cdots, x_r$ 生成的自由群，而且 N 是由所有 $z^n(z \in F_r)$ 生成的完全不变子群，则 $B(n,r) = F_r/N$.

18.2. $n=2$ 和 $n=3$ 时的伯恩赛德问题

如果群 G 的除单位元素外的元素都是 2 阶的，则从 $x^2=$

1) 诺维可夫（П. С. Новиков）在1959年得到了伯恩赛德问题的否定解答（参看 ДАН СССР, 127(1959), 749—752）. ——俄译本编者注

2) 诺维可夫证明，对于 $n \geqslant 72$，存在着无限的有限生成群，它的每个元素的阶都是 n 的约数. ——俄译本编者注

1, $y^2=1$, $(xy)^2=1$ 得出 $xyxy=1$, $xy=y^{-1}x^{-1}=yx$, 因而 G 是阿贝尔群. 因此由 x_1, $\cdots$, x_r 生成而且每个元素的平方等于单位元素的伯恩赛德群 $B(2, r)$ 是以 x_1, $\cdots$, x_r 作为基底的 2^r 阶的阿贝尔群. 这解决了 $n=2$ 的情形.

当 $n=3$ 时,容易证明 $B(3, r)$ 是有限群.我们对 r 施行归纳法. $B(3, 1)$ 是 3 阶循环群. 假设 $B_h=B(3, h)$ 的阶是 $3^{m(h)}$. 我们利用关系

$$yxy=x^{-1}y^{-1}x^{-1}, \tag{18.2.1}$$

这是 $(xy)^3=1$ 的结果. B_{h+1} 从把新生成元素 z 添加到 B_h 而得到. 因此 B_{h+1} 的元素有形状

$$g=u_1z^{\pm 1}u_2z^{\pm 1}\cdots z^{\pm 1}u_n, \tag{18.2.2}$$

这里 $u_i\in B_h$. 我们证明 g 可以最多用两个 z 而表出. 如果在 (18.2.2) 中有相继的两项具有同样的方次数, 我们利用 (18.2.1) 令 $zu_iz=u_i^{-1}zu_i^{-1}$ 或 $z^{-1}u_jz^{-1}=u_j^{-1}zu_j^{-1}$, 因而 z 的个数减去一个. 于是 g 可以表成具有 z 的方次数正负相间的形状 (18.2.2). 这时如果 g 具有三个以上的 z,则当 $g=u_1zu_2z^{-1}u_3z\cdots$时, 我们记$g=u_1zu_2z\cdot zu_3z=u_1u_2^{-1}z^{-1}u_2^{-1}u_3^{-1}zu_3^{-1}\cdots$, 这就使 z 的个数减去一个. 当 $g=u_1z^{-1}u_2zu_3z^{-1}\cdots$ 时可以作同样的论证. 因此 g 可以最多用两个 z 而表出. 我们还可以记 $u_1z^{-1}u_2zu_3=u_1z^{-1}u_2z^{-1}z^{-1}u_3=u_1u_2^{-1}zu_2^{-1}z^{-1}u_3$, 因此 B_{h+1}的每个元素可以具有下列形状中的一个:

$$\begin{aligned}&u_1,\\&u_1zu_2,\\&u_1z^{-1}u_2,\\&u_1zu_2z^{-1}u_3.\end{aligned} \tag{18.2.3}$$

因此 B_{h+1} 最多有 $3^m+2\cdot 3^{2m}+3^{3m}<3^{3m+3}$ 个元素, 所以 $m(h+1)\leqslant 3m(h)$, 因而一般地 $m(r)\leqslant 3^{r-1}$ 而且 $B(3, r)$的阶最多是 $3^{3^{r-1}}$. 伯恩赛德在他原来的文章中用相当复杂的方

法得到更好的限制 $m(r) \leqslant 2^r - 1$. 但是我们要进一步得出确切的结果

$$m(r) = \binom{r}{3} + \binom{r}{2} + r,$$

这是由勒维和范·德·瓦尔登 (Levi and van der Waerden[1]) 得到的.

我们从三次应用 (18.2.1) 的一个公式开始:

$$\begin{aligned} x^{-1}yxzx^{-1} &= (x^{-1}yx^{-1})(x^{-1}zx^{-1}) \\ &= y^{-1}(xy^{-1}z^{-1}x)z^{-1} = y^{-1}zyx^{-1}zyz^{-1}. \end{aligned} \tag{18.2.4}$$

作为 (18.2.4) 的特殊情形,当 $z = y$ 时有 $x^{-1}yxyx^{-1} = yx^{-1}y$, 因而

$$(x^{-1}yx)y = y(x^{-1}yx). \tag{18.2.5}$$

所以元素 y 与它的任何共轭元素可交换. 因此 y 也与 $y^{-1}x^{-1}yx$ 可交换,即用换位子的记号是

$$(y, x, y) = 1. \tag{18.2.6}$$

这还导出

$$\begin{aligned} (x, y)^{-1} &= (x^{-1}y^{-1}xy)^{-1} = y^{-1}x^{-1}yx \\ &= x^{-1}yxy^{-1} = (x, y^{-1}). \end{aligned} \tag{18.2.7}$$

从这些还得出

$$\begin{aligned} (x^{-1}, y) &= (y, x^{-1})^{-1} = (y, x) = (x, y)^{-1}, \\ (y, x, x) &= ((x, y)^{-1}, x) = (x, y, x)^{-1} = 1. \end{aligned} \tag{18.2.8}$$

现在考虑$(a, c, b)^{-1} = b^{-1}(c^{-1}a^{-1}caba^{-1}c^{-1})ac$ 而且在括号中取 $x = c$, $y = a^{-1}$, $z = aba^{-1}$ 而应用 (18.2.4). 这导出

$$\begin{aligned} (a, c, b)^{-1} &= b^{-1}(a \cdot aba^{-1}a^{-1}c^{-1}aba^{-1}a^{-1}ab^{-1}a^{-1})ac \\ &= b^{-1}a^{-1}bac^{-1}aba^{-1}b^{-1}c = (a, b, c). \end{aligned}$$

我们还有 $(a, c, b)^{-1} = ((a, c)^{-1}, b) = (c, a, b)$. 这些结果共同给出

$$(a, b, c) = (c, a, b) = (b, c, a),$$
$$(a, c, b)^{-1} = (a, b, c). \quad (18.2.9)$$

我们现在可以来证明权为 4 的任何换位子都是单位元素.先考虑复合的换位子 $(a, b; c, d)$. 利用(18.2.9),我们有

$$\begin{aligned}(a, b; c, d) &= ((c, d), a, b) = ((c, d, a), b) \\ &= (a, c, d, b) = (a, c, b, d)^{-1} \\ &= ((a, b, c)^{-1}, d)^{-1} = (a, b, c, d).\end{aligned}$$

但是还有 $(c, d; a, b) = ((a, b), c, d) = (a, b, c, d)$. 因此 $(a, b; c, d) = (c, d; a, b) = (a, b; c, d)^{-1}$, 因而

$$(a, b; c, d) = (a, b, c, d) = 1. \quad (18.2.10)$$

根据前面的结果，权为 3 的换位子在包含重复的元素时是单位元素. 至于包含三个不同的生成元素的权为 3 的换位子,则根据(18.2.9)可以写成 (x_1, x_j, x_k), $i < j < k$ 或这个形式的逆. 根据(18.2.10), 权为 3 的换位子属于中心，而且导出群是阿贝尔群. 因此 $B(3, r)$ 的每个元素可以写成:

$$g = x_1^{a_1} \cdots x_r^{a_r} (x_1, x_2)^{b_{12}} \cdots (x_i, x_j)^{b_{ij}} \cdots (x_i, x_j, x_k)^{c_{ijk}}, \quad (18.2.11)$$

这里对于 (x_i, x_j) 有 $i < j$, 对于 (x_i, x_j, x_k) 有 $i < j < k$, 而且方次数是 0, 1 或 2. 这种表达式的总数是 $3^{m(r)}$, 这里

$$m(r) = r + \binom{r}{2} + \binom{r}{3}$$

是从 r 个生成元素 $x_1, \cdots, x_r$ 每取一个，两个或三个的组合数的总和. 因此伯恩赛德群 $B(3, r)$ 的阶不超过 $3^{m(r)}$, 而且只要方次数不都是零的元素(18.2.11)中没有能简化成单位元素的, 这就是确切的阶数. 然而如果两个不同的表达式 g_1 和 g_2 表出 $B(3, r)$ 的同一个元素,则在 $B(3, r)$ 的任何同态像,包括 3^r 阶的初等阿贝尔群里,它们也将如此，因而这两个

表达式的方次数 a_i, $i=1,\cdots,r$ 都相同. 因为导出群是阿贝尔群, $g=g_1g_2^{-1}=1$ 将是表出单位元素的元素, 而它具有某个 b_{ij}或 c_{ijk} 取模 3 时不为零. 把 $g=1$ 看作 $B(3,r)$ 的一个关系, 在添上关系 $x_s=1$, $s\neq i, j, k$ 时它仍然成立. 因此,为了证明 $B(3,r)$ 的确切的阶是 $3^{m(r)}$,只要证明 $B(3,3)$ 的确切的阶是 3^7.

我们利用定理 6.5.1 和 6.5.2 中论述的正规乘积来构造 $B(3,3)$ 作为一个 3^7 阶群. 我们记

$$\begin{aligned} &C_1=x,\ C_2=y,\ C_3=z,\ C_4=(x,y),\\ &C_5=(x,z),\ C_6=(y,z),\ C_7=(x,y,z). \end{aligned} \qquad (18.2.12)$$

先构造 $A=\{C_4, C_5, C_6, C_7\}$ 作为 3^4 阶的初等阿贝尔群. 然后以下列关系把 C_3 添加到A:

$$\begin{aligned} &C_3^3=1,\ C_3^{-1}C_4C_3=C_4C_7,\ C_3^{-1}C_5C_3=C_5,\\ &C_3^{-1}C_6C_3=C_6,\ C_3^{-1}C_7C_3=C_7. \end{aligned} \qquad (18.2.13)$$

根据定理 6.5.1 和 6.5.2, 群 $B=\{A, C_3\}$ 是 3^5 阶的, 而且它是A借助循环群 C_3 的扩张, 只要我们验证: 根据关系(18.2.13), 由 C_3 作变形导出A中的 3 阶的自同构. 用同样的方法,我们可以利用关系

$$\begin{aligned} &C_2^3=1,\ C_2^{-1}C_3C_2=C_3C_6^{-1},\ C_2^{-1}C_4C_2=C_4,\\ &C_2^{-1}C_5C_2=C_5C_7^{-1},\ C_2^{-1}C_6C_2=C_6,\ C_2^{-1}C_7C_2=C_7. \end{aligned} \qquad (18.2.14)$$

借助于 C_2 来扩张 B 而得到 3^6 阶的 $H=\{B, C_2\}$, 最后利用

$$\begin{aligned} &C_1^3=1,\ C_1^{-1}C_2C_1=C_2C_4^{-1},\ C_1^{-1}C_3C_1=C_3C_5^{-1},\\ &\qquad C_1^{-1}C_4C_1=C_4,\\ &C_1^{-1}C_5C_1=C_5,\ C_1^{-1}C_6C_1=C_6C_7,\ C_1^{-1}C_7C_1=C_7, \end{aligned} \qquad (18.2.15)$$

借助于 C_1 把H扩张成 3^7 阶的 $G=\{H, C_1\}$. 根据这些关系, G的幂零类是 3, 而且下列集积公式成立:

$$(PQ)^3=P^3Q^3(Q,P)^3(Q,P,P)(Q,P,Q)^5. \qquad (18.2.16)$$

取 $P=z$ 和 Q 为 A 的任意元素，就得出 B 的方次数[1]是 3. 同理可以证明 H 和 G 的方次数也是 3. 因此 $G=B(3,3)$ 的阶是 3^7. 我们在上面已经指出过，由此就能得出一般的定理.

定理 18.2.1. 伯恩赛德群 $B(3,r)$ 的阶是 $3^{m(r)}$，这里

$$m(r)=r+\binom{r}{2}+\binom{r}{3}.$$

$B(3,r)$ 的元素具有唯一的表达式（18.2.11）.

18.3. $B(4,r)$ 的有限性

伯恩赛德在他最初的论文里证明了 $B(4,2)$ 的阶最多是 2^{12}. 沙诺夫（Sanov [Санов] [1]）证明了 $B(4,r)$ 对于任何 r 都是有限的. 但是除已知 $B(4,2)$ 的阶是 2^{12} 外，$B(4,r)$ 的阶并不确切知道.

定理 18.3.1. 群 $B(4,r)$ 是有限群.

证明. 设 H 是元素的阶都整除 4 的有限群. 我们希望证明，如果把一个 4 阶元素 b 添加到 H，而且要求扩大的群 $G=H\cup(b)$ 的每个元素的四次方幂都等于单位元素，则 G 仍然是有限的. 我们分两步来完成这个扩张，先把 b^2 添加到 H 而产生一个群 $H_1=H\cup(b^2)$，而把 b 添加到 H_1 而产生 $G=H_1\cup(b)=H\cup(b)$. 在这两次扩张中每次都是添加平方属于原先的群的元素. 因此只要证明，如果有限群 H 添加元素 x，这里 $x^2\in H$，而且 $z^4=1$ 对于 $z\in H\cup(x)$，则 $H\cup(x)$ 是有限的.

当 $x^2\in H$ 时，$H\cup(x)$ 的每个元素 g 有形状

1) 指群 B 元素的阶的最小公倍数. 方次数（exponent）也可以译成"指数"，在本书中为了避免与由 index 译成的指数相混，一律把 exponent 译成方次数. ——译者

$$g = h_1xh_2xh_3x\cdots h_{n-1}xh_n,\ h_i \in H. \qquad (18.3.1)$$

从关系 $(xh)^4 = 1$ 得出

$$\begin{aligned} xhx &= h^{-1}x^{-1}h^{-1}x^{-1}h^{-1} = h^{-1}x(x^2h^{-1}x^2)xh^{-1} \\ &= h^{-1}xh^*xh^{-1}, \end{aligned} \qquad (18.3.2)$$

这里 h^* 属于 H. 因此，利用 (18.3.2)，我们可以不增大 (18.3.1) 中的字的长度 n 而把它改变成

$$h_1xh_2\cdots xh_{i-1}h_i^{-1}xh_i^*xh_i^{-1}h_{i+1}x\cdots xh_n. \qquad (18.3.3)$$

如果在 (18.3.1) 中有任何 h_j $(2 \leqslant j \leqslant n-1)$ 是 1，则可以用 $x^2 = h \in H$ 来约简长度. 我们还可以利用 (18.3.2) 几次来把某些 h_j 变成 1.

沙诺夫指出，重复应用 (18.3.2)，我们可以把 h_{i-1} 换成 $h_{i-1}h_i^{-1}$,然而把 h_{i-2} 换成 $h_{i-2}(h_{i-1}h_i^{-1})^{-1} = h_{i-2}h_ih_{i-1}^{-1}$ 等等. 这样我们可以把 h_2 换成 $h_2, h_2h_3^{-1}, h_2h_4h_3^{-1}, h_2h_4h_5^{-1}h_3^{-1}, \cdots, h_2h_4\cdots h_{2s}h_{2s-1}^{-1}\cdots h_3^{-1}$, $h_2h_4\cdots h_{2s}\,h_{2s+1}^{-1}\cdots h_3^{-1}$ 中的一个. 如果其中有一个是 1，则我们就可以约简 g 的长度，而如果H的阶是 M 而且 $n \geqslant M+2$，则或者这些表达式中有一个是 1，或者存在重复的值，例如 $h_2\cdots h_{2r}h_{2r+1}^{-1}\cdots h_3^{-1} = h_2\cdots h_{2r}\cdots h_{2s}h_{2s+1}^{-1}\cdots h_{2r+1}^{-1}\cdots h_3^{-1}$,因而 $h_{2r+2}\cdots h_{2s}h_{2s+1}^{-1}\cdots h_{2r+3}^{-1} = 1$.可是后者是 h_{2r+2} 所能换成的值中的一个. 同理，如果重复的值包括了 $h_2h_4\cdots h_{2r}h_{2r-1}^{-1}\cdots h_3^{-1}$，则 h_{2r+1} 可以换成值为 1 的表达式. 总之当 $n \geqslant M+2$ 时我们可以约简长度. 因此任何 g 都可以用长度 $n \leqslant M+1$ 的字表出. 所以 $H \cup (x)$ 的阶不大于 M^{M+1}.

18.4. 局限的伯恩赛德问题. P. 赫尔和希格曼的定理. $B(6, r)$ 的有限性

伯恩赛德的猜想的较弱的形式是以下的命题；大家把它

叫做局限的伯恩赛德问题:

R_n: 对于每个整数 r, 存在整数 $b_{n,r}$, 使得由 r 个元素生成的方次数 n 的每个有限群的阶不大于 $b_{n,r}$.

即使 R_n 对于某个 n 成立,还可能存在具有 r 个生成元素的方次数 n 的无限群. 但是当 R_n 成立时,就存在由 r 个元素生成的方次数 n 的最大的有限群 $R(n,r)$. 因为由 r 个元素生成的方次数 n 的每个有限群同构于商群 F_r/N_i, 这里 F_r 是具有 r 个生成元素的自由群,N_i 是包含 F_r 的元素的所有 n 次方幂的正规子群. 如果 R_n 成立, 则只能存在有限个这种子群 N_i, 它们的交是有限指数的正规子群 N, 而且 $F_r/N = R(n, r)$ 是由 r 个元素生成的方次数 n 的有限群, 使得所有其他的这种群都是它的同态像.

设 G 是具有下中心序列:

$$G = G_1 \supseteq G_2 \supseteq G_3 \supseteq \cdots \tag{18.4.1}$$

的群. 假定等式 $G_s = G_{s+1}$ 成立. 那么从下中心序列的性质有 $G_s = G_{s+1} = \cdots G_{s+i} = \cdots$. 如果 G 是幂零的, 则有某个 $G_{s+i} = 1$, 因而 $G_s = 1$. 因为方次数为素数方幂 $n = p^t$ 的有限群 G 是幂零群,所以在这种群内从等式 $G_s = G_{s+1}$ 得出 $G_s = 1$. 现在假定 G 的方次数是 p^t, 而且它由 r 个元素生成. 那么每个 G_i/G_{i+1} 都是有限的阿贝尔群. 如果我们能证明,对于这种群 G 存在整数 $s = s(p^t, r)$, 使得 $G_s = G_{s+1}$, 则就解决了方次数 $n = p^t$ 时的局限的伯恩赛德问题.

在应用到 $(xy)^n$ 的集积过程(定理 12.3.1)中, 我们曾经得出

$$(xy)^n = x^n y^n c_1^{a_1(n)} \cdots c_t^{a_t(n)} \cdots, \tag{18.4.2}$$

这里如果 c_i 的权是 m, 则它的方次数 $a_i(n)$ 有形状

$$u_{i1}n + u_{i2}\binom{n}{2} + \cdots + u_{im}\binom{n}{m}. \tag{18.4.3}$$

又如果 c_i 有形状

$$c_i = (y, \overbrace{x, \cdots, x}^{s}), \tag{18.4.4}$$

则方次数 $a_i(n)$ 是这样的指标 $j_1, j_2, \cdots, j_{s+1}$ 的选择数,使得在

$$(y_{j_1}, x_{j_2}, x_{j_3}, \cdots, x_{j_{s+1}}) \tag{18.4.5}$$

中有

$$j_1 < j_2 < j_s < \cdots < j_{s+1}, \tag{18.4.6}$$

而且

$$1 \leqslant j_k \leqslant n.$$

但是这不过是从 1, 2, …, n 中取 $s+1$ 个不同的数的组合数,即是 $\binom{n}{s+1}$.

如果 $n = p$ 是素数,则权不大于 $p-1$ 的换位子的方次数都是 p 的倍数,因为当 $1 \leqslant i \leqslant p-1$ 时的二项式系数 $\binom{p}{i}$ 都是 p 的倍数. 但是对于换位子

$$(y, \overbrace{x, \cdots, x}^{p-1}), \tag{18.4.7}$$

方次数是 $\binom{p}{p} = 1$. 因此在方次数 p 的群 G 内,我们有

$$1 = (xy)^p = (y, \overbrace{x, x, \cdots, x}^{p-1})v_1 \cdots v_t, \tag{18.4.8}$$

这里 $v_1, v_2, \cdots, v_t$ 是权不小于 p 的换位子,而且在权为 p 的换位子中 y 至少出现 2 次.

由此得出在 G_p 取模 G_{p+1} 中的下列等式:

$$(y, \overbrace{x, \cdots, x}^{p-1})v_1 \cdots v_s \equiv 1 (\text{mod } G_{p+1}), \tag{18.4.9}$$

这里 $v_1, \cdots, v_s$ 是以 x 和 y 表出的权为 p 的换位子,而且在其中

x 出现的次数不小于 1 而不大于 $p-2$，根据恒等式 (10.2.1)，在任何群内一般地有：如果 (u, v) 的权是 m，则

$$(u^i, v^j) \equiv (u, v)^{ij} (\mathrm{mod}\ G_{m+1}). \qquad (18.4.10)$$

利用这个我们发现，当 (18.4.9) 中的 v_j 对 x 的权是 r 时，在 (18.4.9) 中把 x 换成 x^i 将把 v_j 换成 $v_j^{i^r}$. 依次令 $i = 1, 2, \cdots, p-1$ 而且把它们乘起来，v_j 在乘积中的方次数满足关系

$$1^r + 2^r + 3^r + \cdots + (p-1)^r \equiv 0\ (\mathrm{mod}\ p), \qquad (18.4.11)$$

这里 $1 \leqslant r \leqslant p-2$，但是对于第一项 $(y, \overbrace{x, \cdots, x}^{p-1})$，$r = p-1$ 而且 $i^r \equiv 1 (\mathrm{mod}\ p)$. 因此上述乘积成为

$$(y, \overbrace{x, \cdots, x}^{p-1})^{p-1} \equiv 1 (\mathrm{mod}\ G_{p+1}), \qquad (18.4.12)$$

因而

$$(y, \overbrace{x, \cdots, x}^{p-1}) \equiv 1 (\mathrm{mod}\ G_{p+1}). \qquad (18.4.13)$$

这个关系曾经是研究方次数为素数 p 的群的局限的伯恩赛德问题的基础. 从这个关系出发，柯斯特里钦 (Kostrikin [Кострикин] [1]) 解决了方次数 5 的具有两个生成元素的群 G 的局限的伯恩赛德问题. 他证明了 $G_{13} = G_{14}$，而且当 G 是有限群时，它的阶不大于 5^{34}.

很多人研究过局限的伯恩赛德问题，这时在与群相结合的李环中进行讨论常常是方便的，下面我们就来描述这个.

设在结合环 R 中用下列规则定义**李乘积** $[x, y]$:

$$[x, y] = xy - yx. \qquad (18.4.14)$$

那么相对于 R 中的加法和李乘积，R 的元素组成李环 L. 李环 L 满足下列定律:

$L0$. **加法** $x + y$ **和李乘积** $[x, y]$ **是有意义的运算.**

$L1$. **在加法下是具有零元素 0 的阿贝尔群.**

$L2.\ [x+y,z]=[x,z]+[y,z]$,

$\quad [x,y+z]=[x,y]+[x,z]$,

$L3.\ [x,x]=0$,

$L4.\ [[x,y],z]+[[y,z],x]+[[z,x],y]=0$,

容易验证由(18.4.14)定义的 $[x,y]$ 满足这些定律.

从 $L2$ 和 $L3$ 得出

$$0=[x+y,x+y]=[x,x]+[x,y]$$
$$+[y,x]+[y,y]=[x,y]+[y,x], \quad (18.4.15)$$

因而

$$[y,x]=-[x,y]. \quad (18.4.16)$$

如果 R 由元素 $x_1, \cdots, x_r$ 生成，则从 $x_1, \cdots, x_r$ 经过加法和李乘积 $[x,y]$ 而生成的元素一般不包括 R 中由加法和原来的结合乘法所生成的全体元素. 由李乘积生成的元素叫做李元素. 例如 x_1^2 不是李元素，而 $x_1^2x_2-2x_1x_2x_1+x_2x_1^2=x_1(x_1x_2-x_2x_1)-(x_1x_2-x_2x_1)x_1$ 是李元素. 当然可以由于 R 中的其他关系而出现 x_1^2 等于一个李元素的情况.

我们可以取定律 $L0$, $L1$, $L2$, $L3$, $L4$ 作为李环 L 的定义. 勃霍夫(Birkhoff[1])和维特(Witt [2])证明，任何李环 L 都能由适当的结合环 R 的李元素组成的环表出. 但是这个重要结果在这里并不需要.

如果 G 是具有下中心序列的群:

$$G=G_1\supseteq G_2\supseteq G_3\supseteq\cdots\supseteq G_n\supseteq\cdots. \quad (18.4.17)$$

对应于 G 的李环 L 以下列方式组成:

1) L 是加法形式的商群 G_i/G_{i+1} 的笛卡儿和，而且 L 的加法就由这个笛卡儿和的加法给出.

2) G_i/G_{i+1} 的元素被认为是次数 i 的齐次元素.

3) 次数 i 的齐次元素 A 和次数 j 的齐次元素 B 的李乘积是取模 G_{i+j+1} 的群换位子 (A, B).

4）L 的一般元素的李乘积由（3）和分配律决定.

我们不证明这些规则定义李环. 我们只指出 $L2$ 相当于换位子的恒等式（10.2.1.2）和（12.2.1.3），而且 $L4$ 相当于（12.2.1.5）. 可以复述 § 11.2 的结果来证明：对应于具有 r 个生成元素的自由群的李环是具有 r 个生成元素的自由李环，只是有些无限和是被允许的. 为了证明这些规则定义李环，可以利用稍加改变的 § 11.2 的方法.

设在李环 L 内把$[x_1, x_2]$记做 x_1x_2，而且递归地把$[x_1, \cdots, x_{n-1}, x_n]$ 记做 $x_1\cdots x_{n-1}x_n$. 我们有属于希格曼（Higmann [1]）的下列定理.

定理 18.4.1. 在对应于素数方次数 p 的群 G 的李环里，关系 $yx^{p-1}=0$ 成立.

证明. 在方次数 p 的群 G 内关系（18.4.13）成立，而且我们把它记做

$$(y, \overbrace{x, \cdots, x}^{p-1}) = c_1c_2\cdots c_t, \qquad (18.4.18)$$

这里 $c_1, c_2, \cdots, c_t$ 是 x 和 y 的总权数，不小于 $p+1$ 的换位子，而且其中 y 的权自然不小于一.

令 $x=x_1x_2\cdots x_{p-1}$，应用公式（10.2.1）来改变（18.4.18）式，使得在左边只留下具有不同的 x_i 的换位子. 那么我们有

$$X=\prod_{\sigma}(y, x_{1\sigma}, \cdots, x_{(p-1)\sigma}) = d_1d_2\cdots d_s, \quad (18.4.19)$$

这里 σ 遍历 $1, 2, \cdots, p-1$ 的 $(p-1)!$ 个置换，而且 $d_1, d_2, \cdots, d_s$ 是这样的换位子，它在 y 中的权是正数，而且或者（1）$y, x_1, \cdots, x_{p-1}$ 的总权数不小于 $p+1$，或者（2）$y, x_1, \cdots, x_{p-1}$ 的总权数是 p，但是有某个 x_j 不出现. 我们不妨假定每个 d_i 在 $y, x_1, \cdots, x_{p-1}$ 的每一个中的权都是正的. 这可以用归纳法证明. 事实上，假定已经有了每个 d_i 在 $y, x_1, \cdots, x_{j-1}$ 中

的权都是正数的这种关系.必要时再导入一些换位子,我们显然可以认为,x_j 中权是零的 d_j 组成开头的一段 $d_1\cdots d_t$,令 $x_j=1$, 就有 $d_1\cdots d_t=1$, 因而它们可以略去. 因此我们可以假定 d_i 在 $y, x_1, \cdots, x_{p-1}$中的权都是正的而且全部权数是 $p+1$. 最初出现的权为 p 的换位子不依赖于某个 x_j, 它将在某一步中排除出去. 而用李环 L 的术语说来, 这是说, 如果 y, x_1, x_2, $\cdots$, x_{p-1} 是任何权的齐次元素,则就有

$$\sum_\sigma yx_{1\sigma}x_{2\sigma}\cdots x_{(p-1)\sigma}=0. \qquad (18.4.20)$$

但是(18.4.20)是在 L 中对齐次元素 y, x_1, $\cdots$, x_p 成立的恒等式.因为它对每个元都是线性的,所以这个恒等式对任何元都成立. 因而当 $x_1=x_2=\cdots=x_p=x$ 而且 y 是任意的时,(18.4.20)成为

$$(p-1)!\,yx^{p-1}=0, \qquad (18.4.21)$$

而且因为 L 的特征是 p, 所以

$$yx^{p-1}=0, \qquad (18.4.22)$$

这就证明了定理.

在特征为 5 (或更进一步是特征与 2 和 3 互素)的李环 L 中利用关系 $yx^4=0$, 希格曼 (Higman [1]) 证明了,如果 L 由 r 个元素生成,则 L 中次数为 Nr 或更高的乘积等于零, 这里 N 是不依赖于 r 的某个整数. 不难指明他事实上已就 $N=25$ 的情形证明了这一点,但是他用进一步的计算指出,他相信可以就 $N=9$ 的情形证明这个结论, 虽然这也许还不是最好的结果.

在一篇重要的论文中, P. 赫尔和希格曼 (P. Hall and Higman [1]) 在得到其他结果的同时,把关于一般方次数的限定的伯恩赛德问题和关于素数方幂方次数的同一问题联系了起来. 但是为此必须限于有限可解群. 这时较 R_n 为弱的猜

想取下列形式:

S_n: 对于每个正整数 r, 存在整数 $b_{n,r}$, 使得由 r 个元素生成的方次数为 n 的每个有限可解群的阶最多是 $b_{n,r}$.

他们的结果可以表述成这样:

定理 18.4.2. 如果 $n = p_1^{e_1}p_2^{e_2}\cdots p_s^{e_s}$ 而且 $S_{p_i^{e_i}}$ 对于 $i = 1, \cdots, s$ 都成立,则 S_n 成立.

我们不在这里给出这个定理的证明，因为它需要一些长而复杂的预备知识. 因为阶为 $p^a q^b$ 的有限群是可解的(定理 16.8.7),所以当 n 最多被两个不同的素数整除时，R_n 和 S_n 意义相同. 而因为已知伯恩赛德群 $B(2, r)$, $B(3, r)$ 和 $B(4, r)$ 是有限的，而且希格曼证明了 R_5 成立，所以定理 18.4.2 指出了 R_6, R_{12}, R_{10}, R_{15}, R_{20} 以及 S_{30} 和 S_{60} 的真实性. 在这些结果的帮助下,作者证明了 $B(6, r)$ 是有限的,下面给出这个证明的概要.

我们将在这里提出 P. 赫尔和希格曼的结果的一小部分，还指出关于其余部分的若干线索.

设 p 是素数，我们把阶与 p 互素的群叫做 p' 群，而且像通常那样把阶为 p 的方幂的群叫做 p 群.

定义. 如果有限群 G 具有正规序列

$$1 = V_0 \subset V_1 \subset \cdots \subset V_n = G, \qquad (18.4.23)$$

其中每个商群 V_{i+1}/V_i 或是 p 群,或是 p' 群，则 G 叫做 p 可解群.

我们从定理 9.2.4 知道,有限可解群 G 对于任何 p 都是 p 可解群,对于 p 可解群 G 我们递归地定义上 p 序列

$$1 = P_0 \subseteq N_0 \subset P_1 \subset N_1 \subset P_2 \subset \cdots \subset P_l \subseteq N_l = G, \quad (18.4.24)$$

要求 N_k/P_k 是 G/P_k 的最大正规 p' 子群，而且 P_{k+1}/N_k 是 G/N_k 的最大正规 p 子群. 使 $N_l = G$ 的最小整数 l 叫做 G 的 p 长度,记做 l_p 或 $l_p(G)$. 容易看出，l_p 是在 G 的(18.4.23)类

型的任何正规序列中的 p 商群的最小个数，这时要求商群 V_{i+1}/V_i 或是 p 群，或是 p' 群.

P. 赫尔和希格曼的论文的目的是连接 p 可解群 G 的 p 长度和 G 的西罗 p 子群 $S(p)$ 的性质. 特别地，设 p^{e_p} 是 $S(p)$ 的方次数，即是 $S(p)$ 的元素的最高阶. 那么 G 的方次数，即 G 的元素的阶的最小公倍数 n，就是 $n=\prod_p p^{e_p}$. 他们的主要定理运用于奇素数 p，而且对于费尔马素数 $p=2^n+1$ 和不是费尔马素数的素数，结果稍有不同. 与伯恩赛德问题密切有关的是下列定理:

定理 18.4.3. 如果 G 是 p 可解群，这里 p 是奇素数，则

1）当 p 不是费尔马素数时有 $e_p \geqslant l_p$,

2）当 p 是费尔马素数时有 $e_p \geqslant \left[\frac{1}{2}(l_p+1)\right]$.

我们可以从定理 18.4.3 导出定理 18.4.2. 设 $n=p_1^{e_1}p_2^{e_2}\cdots p_s^{e_s}$. 当 n 是偶数时可以取 $p_1=2$，然后对 s 施行归纳法，假设 S_m 对于 $m=p_1^{e_1}p_2^{e_2}\cdots p_{s-1}^{e_{s-1}}$ 成立. 那么根据定理 18.4.3，方次数 n 的有限可解群 G 的 p_s 长度不大于 $2e_s$: $l=l_{p_s}\leqslant 2e_s$. 于是当 G 由 r 个元素生成时，根据 S_m，G/P_l 的阶不大于 $b_{m,r}$，因而（根据引理 7.2.2 的推论）P_l 的生成元素的个数是有限的，设是 r_1. 然后根据 $S_{p_s^{e_s}}$，P_l/N_{l-1} 的阶有界而且 N_{l-1} 的生成元素的个数有界. 这样继续下去，每个 N_i/P_i 和 P_i/N_{i-1} 的阶都以某个 $b_{m,k}$ 或 $b_{p_s^{e_s},k}$ 为界，因此由于 $l\leqslant 2e_s$，我们得出 G 的阶有界.

定理 18.4.4. 在有限 p 可解群 G 的上 p 序列

$$1=P_0\subseteq N_0\subset P_1\subset N_1\subset P_2\subset\cdots\subset P_l\subseteq N_l=G$$

中，P_1/N_0 包含着它在 G/N_0 内的中心化子.

推论 18.4.1. P_1 包含着它在 G 内的中心化子.

推论的证明. 如果 x 属于 P_1 在 G 内的中心化子，则 xN_0/N_0 属于 P_1/N_0 在 G/N_0 内的中心化子. 因此根据定理，xN_0/N_0 属于 P_1/N_0，因而在 G 内，傍系 xN_0 包含在 P_1 内，所以 x 属于 P_1.

定理的证明. 在群 $G_1 = G/N_0$ 内不存在正规 p' 子群，因为 N_0 是 G 的最大的正规 p' 子群. G_1 的子群 $\bar{P}_1 = P_1/N_0$ 根据它的构成是 G_1 的最大的正规 p 子群. 设 Z 是 $\bar{P}_1$ 在 G 内的中心化子，而且假定与定理的轮断相反，$Z \nsubseteq \bar{P}_1$. 因为 Z 是 G_1 的正规子群，所以 $Z \cup \bar{P}_1 = Z\bar{P}_1$ 是 G_1 的正规子群. 我们假定了 $Z\bar{P}_1 \supset \bar{P}_1$，设 M 是使 $\bar{P}_1 \subset M \subseteq Z\bar{P}_1$ 的 G_1 的极小正规子群. 那么 $M/\bar{P}_1$ 不会是 p 群，因为 $\bar{P}_1$ 是 G_1 的极大正规 p 子群. 于是因为 G 是 p 可解的，所以 $M/\bar{P}_1$ 是 p' 子群. 于是 $\bar{P}_1$ 和 $M/\bar{P}_1$ 的阶互素，而且根据定理 15.2.2，M 在 $\bar{P}_1$ 上可裂，即 $M = K\bar{P}_1$，这里 $K \cap \bar{P}_1 = 1$ 对于 M 的同构于 $M/\bar{P}_1$ 的子群 K. 因为 $K \subseteq Z\bar{P}_1$，用 K 的元素 y 作 $\bar{P}_1$ 的变形导出 $\bar{P}_1$ 的内自同构，而且因为 K 和 $\bar{P}_1$ 的阶互素，这个内自同构只能是恒同自同构. 因此 M 是 K 和 $\bar{P}_1$ 的直积，$M = K \times \bar{P}_1$. 于是 K 作为 M 的特征子群，它是 G_1 的正规子群，这与 G_1 不包含正规 p' 子群的事实矛盾. 总之，$Z \nsubseteq \bar{P}_1$ 的假设引出了矛盾，我们的定理也就证明了.

下一步主要是改善前一个定理.

定理 18.4.5. 如果 G 是具有上 p 序列

$$1 = P_0 \subseteq N_0 \subset P_1 \subset N_1 \subset P_2 \subset \cdots \subset P_l \subseteq N_l = G$$

的 p 可解群，而且 F/N_0 是 P_1/N_0 的弗拉梯尼子群，则由 G 的元素作变形而导出的 P_1/F 的自同构一一地表示了 G/P_1.

证明. F/N_0 是 p 群 P_1/N_0 的极大子群的交，而且 P_1/F 是初等阿贝尔 p 群(定理 12.2.1). 因为 F/N_0 包含 P_1/N_0 的导出群，所以用 P_1 的任何元素作变形时导出 P_1/F 的恒同自

同构，因此，G 的导出 P_1/F 的恒同自同构的元素的集合是 G 的子群 K（必定在 G 内正规），而且 $K \supseteq P_1$. 我们来证明 $K \supset P_1$ 将引出矛盾，因而 $K = P_1$，于是 G/P_1 就由 P_1/F 的内自同构一一地表示. 如果 $K \supset P_1$，则 K/P_1 不是 p 群. 因为根据构成，P_1/N_0 是 G/N_0 的极大正规 p 子群. 于是 K 包含不属于 P_1 的元素 x，它的阶与 p 互素，而且用它作变形导出 P_1/F 的恒同自同构. 但是根据 12.2.2，p 群 P_1/N_0 的自同构当在 P_1/F 上是恒同自同构时，它的阶是 p 的方幂. 于是因为 x 的阶与 p 互素，x 导出 P_1/N_0 的恒同自同构，而且根据定理 18.4.4，这说明 $x \in P_1$，这与 x 的选取矛盾. 总之 $K \supset P_1$ 的假设引出矛盾，因而 $K = P_1$，定理也就证明了.

根据定理 18.4.5，群 G/P_1 被初等阿贝尔群 P_1/F 的自同构所一一表示. 这时 G/P_1 是 p 可解群而且 $l_p(G/P_1) = l_p(G) - 1$. 其次，根据定义，G/P_1 不包含正规 p 子群. P. 赫尔和希格曼的论文的其余部分研究了 G/P_1 在 P_1/F 上的表示的性质，即事实上是以 p 个元素的域上的向量空间的线性变换来表示. G/P_1 是不包含正规 p 子群的 p 可解群. 进一步的理论取决于下列事实：关于可以具有特征 p 的域上的一一表示的群能说些什么. 得到这些结果还要利用 $l_p(G) = l_p(G/P_1) + 1$ 而对 p 长度施行归纳法.

不考虑上述结果，我们限于讨论方次数 6 的有限群 G，以便在能证明伯恩赛德群 $B(6, r)$ 是有限群时决定它们的本质.

定理 18.4.6. 在方次数 6 的有限群 G 内，$l_2(G) \leqslant 1$ 而且 $l_3(G) \leqslant 1$.

证明. 方次数 6 的有限群 G 的阶必定是 2^a3^b，因而它是可解的. 在 G 的上 2 序列中，P_1/N_0 是包含着它在 G/N_0 内的中心化子的 2 群. 而因为 G 的方次数是 6，又 G 的西罗 2

子群的方次数是 2，因而它是初等阿贝尔群．因此，G/N_0 的西罗 2 子群包含在 P_1/N_0 的中心化子内，因而它包含在 P_1/N_0 内． 于是 P_1/N_0 是 G/N_0 的西罗 2 子群，所以 $l_2(G)=1$，而且 G 的上 2 序列有形状:

$$1=P_0\subseteq N_0\subset P_1\subseteq N_1=G, \qquad (18.4.25)$$

这里 N_0/P_0 是 3 群; P_1/N_0 是 2 群; N_1/P_1 是 3 群.

因为 (18.4.25) 是 G 的正规序列，其中最多有两个商群是 3 群，所以 $l_3(G)\leqslant 2$. 我们来证明，从 $l_3(G)=2$ 将得出 G 包含 9 阶元素，这与 G 的方次数是 6 相矛盾，这样就有结论 $l_3(G)\leqslant 1$. 上 3 序列有形状

$$1=A_0\subseteq B_0\subset A_1\subset B_1\subset A_2\subseteq B_2=G, \qquad (18.4.26)$$

这里 B_0/A_0, B_1/A_1, B_2/A_2 是 2 群，A_1/B_0 和 A_2/B_1 是 3 群. 我们注意到

$$1=B_0/B_0\subset A_1/B_0\subset B_1/B_0\subset A_2/B_0\subseteq G/B_0 \qquad (18.4.27)$$

是 G/B_0 的上 2 序列，而且因为它的 2 长度是 1，所以 $A_2=B_2=G$，根据定理 18.4.4，2 群 B_1/A_1 是它自己在 A_2/A_1 内的正规化子，因此，对于在 A_2/A_1 内给定的 3 阶元素 x，在 B_1/A_1 内存在 2 阶元素 u，使得 x 和 u 不可交换，如果我们记

$$u=u_1,\ x^{-1}u_1x=u_2,\ x^{-1}u_2x=u_3, \qquad (18.4.28)$$

则因为 $x^3=1$ 而有 $x^{-1}u_3x=u_1$. 令 $y=y_1=u_1u_2$ 和 $y_2=u_2u_3$. 因为 u_1, u_2, u_3 属于初等阿贝尔 2 群，所以 $u_3u_1=(u_1u_2)\cdot(u_2u_3)=y_1y_2$. 因此群 $C=\{x,y_1,y_2\}$ 满足关系

$$x^3=1,\ y_1^2=y_2^2=1,\ y_2y_1=y_1y_2, \qquad (18.4.29)$$
$$x^{-1}y_1x=y_2,\ x^{-1}y_2x=y_1y_2.$$

因为 x 与 u_1, $u_2\neq u_1$ 不可交换，所以 $y_1=u_1u_2\neq 1$. 又如果 $y_2=y_1$，则 $x^{-1}y_2x=1$ 和 $1=y_2=y_1$. 因此 $y_2\neq y_1$，于是根据关系(18.4.29)可知群 C 是 12 阶的，而且它实际上同构于四个文字上的交替群. 根据定理 18.4.5，如果 F/B_0 是 A_1/B_0 的

弗拉梯尼子群，则 G/A_1 由初等阿贝尔 3 群 A_1/F 的变形一一地表示. 特别地，C 由 $A_1/F = W$ 的变形一一地表示. 如果W用加法表出，则用 G/A_1 的元素 z 作W的变形可以表成取 z 作为作用于右侧的算子. 这时作用于W的不仅是群 C，而且是群环 C^*. 容易验证，C^* 中把W的每个元素都映成零的算子组成 C^* 的双侧理想. 我们把C看做由 x 和 $y = y_1$ 按照下列关系生成:

$$x^3 = 1,\ y^2 = 1,\ (xy)^3 = 1. \tag{18.4.30}$$

那么 C^* 的包含 $1 + x + x^2$ 的双侧理想也包含

$$\begin{aligned} & x^2y(1 + x + x^2)yx - (1 + x + x^2)y \\ & - y(1 + x + x^2) + xy(1 + x + x^2)yx^2 \\ & = 2 - 2y. \end{aligned} \tag{18.4.31}$$

如果对于每个 $w \in W$ 有 $w(1 + x + x^2) = 0$，则根据(18.4.31)，我们还将有 $w(2 - 2y) = 0$，于是因为W的元素是 3 阶的，这说明对于每个 $w \in W$ 都有 $wy = w$. 于是 y 不能由 $W = A_1/F$ 的变形一一表示，这就与定理18.4.5矛盾.因此，对于某个 $w \in W$ 有 $w(1 + x + x^2) \neq 0$.用乘法写出时这是说，对于作为 A_2/A_1 的元素 x 的傍系 $\bar{x}A_1$ 的代表 $\bar{x}$，我们有

$$w(\bar{x}^{-1}w\bar{x})(\bar{x}^{-2}w\bar{x}^2) \neq 1. \tag{18.4.32}$$

而这正是元素

$$(w\bar{x}^{-1})^3\bar{x}^3 \neq 1. \tag{18.4.33}$$

$\bar{x}^3$ 和 $(w\bar{x}^{-1})^3$ 都是W的元素. 根据(18.4.33)，这两个元素都不能是单位元素. 因此 $\bar{x}$ 或 $w\bar{x}^{-1}$ 有一个是 9 阶元素. 总之 $l_3(G) = 2$ 导出 9 阶元素的存在而与G的方次数是 6 相矛盾. 因此 $l_3(G) \leqslant 1$，定理也就证明了.

利用定理 18.4.6，我们可以找到由 r 个元素生成的方次数为 6 的最大的有限群的确切的阶.

定理 18.4.7. 群 $R(6, r)$ 的阶是

$$2^a 3^{b+\binom{b}{2}+\binom{b}{3}}, \quad (18.4.34)$$

这里

$$a = 1 + (r-1)3^{r+\binom{r}{2}+\binom{r}{3}}, \ b = 1 + (r-1)2^r.$$

证明. 设 F_r 是具有 r 个生成元素的自由群. 如果 S 是由 F_r 的元素的平方生成的群, 则 F_r/S 是 2^r 阶的初等阿贝尔群. 因此根据定理 7.2.8, S 是具有 $b = 1 + (r-1)2^r$ 个生成元素的自由群. 由 S 的元素的立方生成的完全不变子群 T 使得 S/T 是 $B(3, b)$, 因而 T 在 S 内的指数是 $3^{b+\binom{b}{2}+\binom{b}{3}}$. 这时 F_r/T 是方次数 6 的有限群,因为对于 $g \in F_r$, $g^2 \in S$ 而且 $(g^2)^3 \in T$. 同理, 由 F_r 的元素的立方生成的子群 C 在 F_r 内的指数是 $3^{r+\binom{r}{2}+\binom{r}{3}}$,而且根据定理 7.2.8, C 有 $a = 1 + (r-1)3^{r+\binom{r}{2}+\binom{r}{3}}$ 个自由生成元素. 由 C 的元素的平方生成的完全不变子群 D 在 C 内的指数是 2^a. 现在设 $X = D \cap T$. F_r/X 是方次数 6 的有限群, 因为对于每个 $g \in F_r$, D 和 T 都包含着 g^6. 容易得出 F_r/X 的上 2 序列是

$$1 = X/X \subset D/X \subset C/X \subset F_r/X, \quad (18.4.35)$$

而且 F_r/X 的上 3 序列是

$$1 = X/X \subset T/X \subset S/X \subset F_r/X. \quad (18.4.36)$$

这时 C/D 和 S/T 分别同构于 F_r/X 的西罗 2 子群和西罗 3 子群,因而 F_r/X 的阶是(18.4.34)中的数.

设 G 是由 r 个元素生成的方次数 6 的有限群. 那么如果

$$1 = P_0 \subseteq N_0 \subseteq P_1 \subseteq N_1 = G \quad (18.4.37)$$

是 G 的上 3 序列, 则 N_1/P_1 的阶最多是 2^r, 于是 P_1 最多由 b 个元素生成,因而同构于 G 的西罗 3 子群的 P_1/N_0 的阶最多是 $3^{b+\binom{b}{2}+\binom{b}{3}}$. 同理, G 的阶最多被 2^a 整除.

要完全证明关于方次数 6 的伯恩赛德猜想需要作很长的

计算，这里不预备做这工作了．这个证明并不用到前面的结果，而且它指出整除 $B(6, r)$ 的阶的 2 的方幂，但是为了得出 3 的方幂，必须应用定理 18.4.7．证明的内容是：指出方次数为 6 的有限生成群 G 的 2 长度是 1，因而根据 $B(2, r)$ 和 $B(3, r)$ 的有限性，G 是有限的．这就是要证明下列正规链的存在

$$G \supset M \supset M' \supset 1, \qquad (18.4.38)$$

这里 G/M 是有限 3 群，M/M' 是有限 2 群，M' 是方次数 3 的有限生成群因而是有限群．困难几乎全在于证明 M' 的方次数是3．

定理 18.4.8. 由 r 个元素生成的方次数 6 的群 G 是有限的．

推论 18.4.2. 群 $B(6, r)$ 的阶等于 (18.4.34) 的数．

引理 18.4.1. G 的元素的立方生成指数最多是 $3^{r+\binom{r}{2}+\binom{r}{3}}$ 的正规子群 M．

引理 18.4.2. M 由有限个 2 阶元素生成．M 的导出群 M' 在 M 内的指数是 2 的方幂，而且 M' 由有限个形状 $abab$ 的元素生成，这里 $a^2 = b^2 = 1$．

引理 18.4.3. 如果群 H 由 $x_1, \cdots, x_n$ 生成，而且 H 的由四个 x_i 生成的任何子群的方次数是 3，则 H 的方次数是 3．

引理 18.4.4. 如果 $H = \{a, b, c, d\}$ 的方次数是 6，而且 $\{a, b, c\}, \{a, b, d\}, \{a, c, d\}$ 和 $\{b, c, d\}$ 的方次数是 3，则 H 的方次数是 3．

引理 18.4.5. 如果 $H = \{x, a, b\}$ 的方次数是 6，而且 $x^2 = 1$, $a^3 = b^3 = 1$, $xax = a^{-1}$, $xbx = b^{-1}$，则 $\{a, b\}$ 的方次数是 3．

这是最困难的引理，在证明时需要从定义关系进行一些复杂的推导．

引理 18.4.6. 如果 $H=\{x, a, b\}$ 的方次数是 6，而且 $x^2=1$, $a^3=b^3=1$, $xax=a^{-1}$, $xbx=b$, 则 $\{a, b\}$ 的方次数是 3.

引理 18.4.7. 如果 $H=\{x, a, b, c\}$ 的方次数是 6, 而且 $x^2=1$, $a^3=b^3=c^3=1$, $xax=a^{-1}$, $xbx=b^{-1}$, $xcx=c^{-1}$, 则 $\{a, b, c\}$ 的方次数是 3.

引理 18.4.8. 如果 $H=\{x, a_1, \cdots, a_n\}$的方次数是 6, 而且 $x^2=1$, $a_i^3=1$, $xa_ix=a_i^{-1}$, $i=1, \cdots, n$,则 $\{a_1, \cdots, a_n\}$ 的方次数是 3.

容易看出这个引理从引理 18.4.3, 18.4.4 和 18.4.7 得出.

引理 18.4.9. 如果 $H=\{a, b, c\}$ 的方次数是 6，而且 $a^2=b^2=c^2=1$, 则 H' 的方次数是 3.

引理 18.4.10. 如果 $H=\{a, b, c, d\}$的方次数是 6, 而且 $a^2=b^2=c^2=d^2=1$, 则 $\{abab, cdcd\}$ 的方次数是 3.

引理 18.4.11. 如果 $H=\{a, b, c, d, e, f\}$ 的方次数是 6, 而且 $a^2=b^2=c^2=d^2=e^2=f^2=1$,则 $\{abab, cdcd, efef\}$ 的方次数是 3,

引理 18.4.12. 群 M' 的方次数是 3，因而它是有限的. 因此群 G 是有限的.

这个引理是引理 18.4.2,18.4.3, 18.4.4 和 18.4.11 的直接结果.

第十九章 子 群 的 格

19.1. 一 般 性 质

群 G 的子群在并和交的运算下可以看作一个格 $L(G)$ 的元素. 素数阶的循环群的子群只有整个群和单位元素子群，因而所有这种群有相同的子群格，它单由两个元素的链组成. 我们曾经证明过(定理 1.5.4)，反之，没有真子群的群是单位元素群或素数阶的有限循环群. 我们还知道，阶为 pq，$p<q$，$p|q-1$ 的非阿贝尔群和阶为 q^2 的初等阿贝尔群有相同的子群格，它由单位元素群. $q+1$ 个素数阶子群和整个群组成，这时任何两个真子群的交是单位元素群而且它们的并是整个群.

因此，虽然 G 唯一决定 $L(G)$，但是一般说 $L(G)$ 不唯一决定 G. 其次，容易找出不是任何群 G 的子群格 $L(G)$ 的格来. 但是有很多群 G 却被 $L(G)$ 唯一决定，例如四个文字上的交替群和对称群就是如此，甚至可以这样说，除少数结构较为简单的群以外，$L(G)$ 唯一决定 G.

从格论术语说，$L(G)$ 是完全的. 这是说总存在无限的并和交，因为一族子群中全体子群的公共元素组成群，它就是这族子群的交，又从一族子群取的元素的有限乘积组成群，它就是这族子群的并.

关于子群格的较完全的讨论，请读者参看铃木通夫的书(Suzuki[1]).

19.2. 局部循环群和分配格

在格内两个分配律

$D1.\ a\cap(b\cup c)=(a\cap b)\cup(a\cap c)$,

$D2.\ a\cup(b\cap c)=(a\cup b)\cap(a\cup c)$

是彼此等价的. 我们来证明从 $D1$ 得出 $D2$. 这时利用 $D1$,

$$\begin{aligned}(a\cup b)\cap(a\cup c)&=[(a\cup b)\cap a]\cup[(a\cup b)\cap c]\\&=a\cup[(a\cap c)\cup(b\cap c)]\\&=[a\cup(a\cap c)]\cup(b\cap c)\\&=a\cup(b\cap c),\end{aligned}$$

这就是 $D2$. 同理可以从 $D2$ 得出 $D1$. 在格中分配律是极强的条件. 我们来证明,对于群 G 说, $L(G)$ 可分配是极强的条件,而且由此得出 G 是局部循环的.

定义. 群 G 是局部循环群, 必要而且只要 G 中任何有限个元素生成循环群. (请与 § 13.1 比较.)

因为阶大于 1 的有限阶元素不能和无限阶元素共同生成循环群, 所以在局部循环群内或者每个 $\neq 1$ 的元素都是无限阶的,或者都是有限阶的, 有理数加法群 R_+ 是非周期的局部循环群,群 R_+ 取模 1 是周期的局部循环群. 不难证明, 局部循环群是这两个群中一个的子群.

定理 19.2.1. 格 $L(G)$ 是可分配的, 必要而且只要 G 是局部循环群.

证明. 我们先假定 G 是局部循环群. 设 A, B, C 是 G 的任意三个子群. 我们来证明 $D1$ 成立. 但是一般地说

$$A\supseteq A\cap B,$$

$$B\cup C\supseteq B\supseteq A\cap B,$$

因而 $U=A\cap(B\cup C)\supseteq A\cap B$. 再有

$$A \supseteq A \cap C,$$

$$B \cup C \supseteq C \supseteq A \cap C,$$

因而 $U = A \cap (B \cup C) \supseteq A \cap C$. 联合这两个包含式，

$$U = A \cap (B \cup C) \supseteq (A \cap B) \cup (A \cap C).$$

所以只需要证明包含式

$$U = A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C) = V,$$

现在考虑任意元素 $g \in U$, 这时 g 有形状

$$g = a = bc, \ a \in A, \ b \in B, \ c \in C,$$

这里因为 G 是阿贝尔群，所以 $B \cup C = BC$. 因为 G 是局部循环的,元素 b 和 c 生成循环群 $\{u\}$, 因而 $u^r = b$, $u^s = c$, 又因为对于某个 m 和 n, $b^m c^n = u$, 所以 $u^{rm+sn} = u$. 再有 $a = bc = u^{r+s}$. 现在 $x = a^{r(r+s)} = a^r = b^{r+s} \in A \cap B$ 而且 $y = u^{s(r+s)} = a^s = c^{r+s} \in A \cap C$. 因此 $a = u^{r+s} = u^{mr(r+s)+ns(r+s)} = x^m y^n$ 是 $(A \cap B) \cup (A \cap C)$ 的元素，这就是要求证明的. 总之,在所有情形下,对于局部循环群的子群都有

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

现在来证明逆命题,假定 $L(G)$ 是可分配的,因而同时满足 $D1$ 和 $D2$, 设 b 和 c 是 G 的两个元素而且记 $a = bc$ 和

$$A = \{a\}, \ B = \{b\}, \ C = \{c\}.$$

那么因为 $a \in B \cup C$, 所以

$$A = A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

作为循环群的子群, $A \cap B$ 和 $A \cap C$ 都是循环群,设

$$A \cap B = \{u\}, \ A \cap C = \{v\},$$

这时对于适当的方次数有

$$a^x = b^y = u, \ a^z = c^w = v,$$

这里 u 和 v 作为 a 的方幂是可交换的，而且因为 $A = \{u\} \cup \{v\}$, $a \in A$, 我们必定有 $a = u^r v^s = u^s v^r$, 而由于 $a = bc$, 所以 $bc = u^r v^s = b^{yr} c^{ws} = c^{ws} b^{yr}$. 于是 $b^{1-yr} = c^{ws-1}$, 因而

$c^{-uvs+1} = b^{yr-1}$或$v^{-s}c = u^r b^{-1}$，因而 $cb = v^s u^r = u^r v^s = bc$. 因此 b 和 c 可交换，即G是阿贝尔群.

我们再来证明G不能同时包含有限阶的元素 $a \neq 1$ 和无限阶的元素 b. 因为令 $c = ab$, c 也是无限阶的，而且 $\{a\} = \{a\} \cap (\{b\} \cup \{c\})$，因为 $a = b^{-1}c$，然而 $(\{a\} \cap \{b\}) \cup (\{a\} \cap \{c\}) = (1) \cup (1) = 1 \neq \{a\}$，因为不包含 $\neq 1$ 的有限阶元素的无限循环群$\{b\}$和$\{c\}$必定与$\{a\}$相交于单位元素群. 因而我们只需要讨论两种情形，第一，G是非周期的，第二，G是周期的. 不论哪一种情形，如果有两个元素不生成周期群，则根据关于阿贝尔群的基本定理，它们生成两个循环群（例如$\{b\}$和$\{c\}$）的直积，这时由于 $a = bc$ 和 $A = \{a\}$，$B = \{b\}$，$C = \{c\}$，我们有 $A = A \cap (B \cup C)$ 和 $(A \cap B) \cup (A \cap C) = (1) \cup (1) = (1)$，因而$D1$不成立. 在周期群的情形，如果 b 和 c 有互素的阶，则 $\{b\} \cup \{c\} = \{bc\}$，它们生成循环群，而当$\{b\}$和$\{c\}$的阶有一个公约数是素数 p 时，它们的直积将不具有可交换的子群格，因为对于 p 阶的 $b_1 \in \{b\}$ 和 $c_1 \in \{c\}$ 以及 $a_1 = b_1 c_1$，$A = \{a_1\}$，$B = \{b_1\}$ 和 $C = \{c_1\}$ 像上面一样地不满足分配律. 因而分配律成立的必要条件仍然是任何两个元素生成一个循环群. 而如果任何两个元素都生成循环群，则立刻得出任何有限个元素生成循环群，因而G是局部循环的，这就证明了定理中的逆命题.

19.3. 岩泽定理

在 § 8.4 里证明过的合成序列（或主序列）的一个性质是全体序列有相同的长度. 这个性质是正规子群格的模性和合成序列中模性的一个弱形式的结果. 但是一般地说，未加限制的子群的极大链长度可以不同. 根据定理 10.5.6，由此得

出在有限超可解群内，子群的极大链有相同的长度．下列属于岩泽（Iwasawa[1]）的定理证明逆命题也成立．

定理 19.3.1. 有限群 G 的极大子群链全都具有相同的长度，必要而且只要 G 是超可解的．

证明. 上面说过，定理 10.5.6 指出，在超可解群 G 内，所有极大子群链具有相同的长度，这就是整除 G 的阶的素数（重复的照算）的总个数．

让我们把所有极大链具有相同的长度的性质叫做等链条件．这个性质显然为子群和商群所继承．设 G 是具有等链性的有限群．因为当群的格是长度为 1 的链时，这群是素数阶的循环群，因而是超可解的，所以我们可以对极大链的长度作归纳假设：G 的全体子群和商群都是超可解的．

我们先来证明关于超可解群的一个引理．

引理 19.3.1. 设 G 是阶为 $n=p_1p_2\cdots p_m$ 的有限超可解群，这里 $p_1\leqslant p_2\leqslant\cdots\leqslant p_m$. 那么 G 具有主序列

$$K_0=1\subset K_1\subset K_2\subset\cdots\subset K_m=G,$$

这里 K_i/K_{i-1} 的阶是 p_{m-i+1}，$i=1,\cdots,m$.

这是推论 10.5.2

证明的极为困难的下一步是指出 G 具有正规子群．为此需要一种选择方法．引理 19.3.2 保证这种选择对于任何有限群是可解的．

引理 19.3.2. 如果 G 是阶能被素数 p 整除的有限群，则或者 (1) G 是 p 正规的，或者 (2) G 具有阶为 p 的方幂的子群 P，它在一个西罗子群 $S_1(p)$ 内是正规的，而在另一个西罗子群 $S_2(p)$ 内不是正规的．

证明. 我们知道，按照定义，群 G 是 p 正规的，假如西罗子群 $S_1(p)$ 的中心 Z 是任何别的包含它的西罗子群 $S_2(p)$ 的中心．因此如果 G 不是 p 正规的，则某个 $S_1(p)$ 的中心 Z 包含

在另一个$S_2(p)$内，而不是$S_2(p)$的中心．在这个情形下我们来证明第二种可能性成立，这时取P作为Z来证明Z在$S_2(p)$内不是正规的． 假定相反地，Z在$S_2(p)$内是正规的，那么$S_1(p)$和$S_2(p)$都包含在$N=N_G(Z)$内，因而它们作为N的西罗子群在N内是共轭的．因此对于某个$x\in N$，$x^{-1}S_1(p)x=S_2(p)$．因为Z是$S_1(p)$的中心，所以$S_2(p)=x^{-1}S_1(p)x$的中心是 $x^{-1}Zx=Z$，这是由于 $x\in N_G(z)$． 这结论与z不是$S_2(p)$的中心的假设矛盾．这就证明了引理．我们注意到在第二种情形里可以应用伯恩赛德定理 4.2.5．

设我们的群G的阶是 $n=p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$，这里 $p_1<p_2<\cdots<p_r$是不同的素数．我们对于整除n的最小素数p_1利用引理 19.3.2． 我们来证明在G内不能出现第二种情形．这时根据定理 4.2.5，存在$t\not\equiv 0(\mathrm{mod}\,p_1)$个$p_1$群 h_1，h_2，$\cdots$，h_t，在它们的并H内是正规的，而且在H对G的正规化子 $N=N_G(H)$内是共轭的．如果H在G内是正规的，则我们就有了希望得到的正规子群． 假定N是G的真子群，因而根据归纳假设是超可解的． 对N应用引理 19.3.1，我们发现N有正规子群Q，它在N内的指数是p_1的整除N的阶的最高方幂．于是Q和H都是N的正规子群，又因为$Q\cap H=1$(H是p_1群)，所以$Q\cup H=Q\times H$．因此Q与H的每个元素可交换，所以h_1的正规化子包含Q，因而不能有与p_1互素的指数 t． 严格地说，我们证明了的只是当N是正规子群时第二种情形不能出现，但是当我们最终地证明了G是超可解群时，上面的论证对于$N=G$也成立．

现在我们考虑第一种可能情形，即G是p_1正规的．设Z是西罗子群$S_1(p_1)$的中心． 设$K=N_G(Z)$． 如果$K=G$，则Z是G的正规真子群．这就是要求证明的． 因此假定K是G的真子群，因而根据归纳假设是超可解的． 于是把引理

19.3.1 应用于 K，K 必定有指数为 p_1 的正规子群 W，而且因为 K/W 是 p_1 阶的循环群，$W \supseteq K'$，K 有一个非显然的同态像是阿贝尔 p_1 群，我们把它记做 $K/K'(p_1)$. 但是根据定理 14.4.5，因为 G 是 p_1 正规的，所以 $G/G'(p_1)$ 同构于 $K/K'(p_1)$，因而 $G'(p_1)$ 是正规的真子群. 因为在所有情形都证明了 G 具有正规的真子群，又因为根据归纳假设，正规子群和商群都是超可解的，所以 G 是可解的.

总之当 G 的阶是 $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$，$p_1 < p_2 < \cdots < p_r$，而且 $m = e_1 + e_2 + \cdots + e_r$ 时，已经证明 G 是可解的，现在我们知道所有极大链的长度都是 m，而且每个盖住关系 $A > B$ 都有 $[A:B]$ 是素数. 设 $S(p_r)$ 是 $p_r^{e_r}$ 阶的西罗子群，再设 $1 \subset A_1 \subset A_2 \subset \cdots \subset A_{e_r} = S(p_r) \subset B_1 \subset \cdots \subset B_{m-e_r} = G$ 是极大链，它包含 $S(p_r)$ 的极大链作为开头部分，我们希望证明 $S(p_r)$ 在 G 内是正规的. 这时 $B_1/S(p_r)$ 的阶是素数 $p_j < p_r$. 因为 $S(p_r)$ 在 B_1 内的共轭群的个数整除 p_j 而且根据第三个西罗定理有形状 $1 + kp_r$，这个数只能是 1，因而 $S(p_r) \triangleleft B_1$. 同理，如果我们证明了 $S(p_r)$ 在某个 B_i 内是正规的，则 $S(p_r)$ 在 B_{i+1} 内的共轭群的个数有形状 $1 + kp_r$ 而且也是 $[B_j + 1: B_i] = p_j < p_r$ 的约数. 因此 $S(p_r)$ 在 B_{i+1} 内是正规的. 继续这个论证，最后得出 $S(p_r) \triangleleft G$. 因为 G 是可解群，所以它具有 $S(p_r)$ 的西罗补群 C，C 的阶是 $p_1^{e_1} \cdots p_{p-1}{}^{e_{r-1}}$. 这是由定理 9.3.1 给出的. 设 Z 是 $S(p_r)$ 的中心. 作为 $S(p_r)$ 的特征子群，Z 在 G 内是正规的. 因此 $C \cup Z = CZ = U$. 在 U 内 C 的极大链可以扩大成 U 的极大链，而在这链内，对于使 $[V: C] = p_r$ 的群 V 有 $C \subset V$. 根据证明 $S(p_r)$ 在 G 内正规的同样论证，可以得出 V 具有阶为 p_r 的正规子群 R. 这时 R 必定包含在 Z 内，Z 是 U 内关于 p_r 的唯一西罗子群. 因而 R 属于 C 的正规化子，而且由于它属于 $S(p_r)$ 的中心，所以也属于

$S(p_r)$的正规化子. 因此R在G内是正规的. 在证明了G具有素数阶p_r的正规子群以后，因为根据归纳假设G/R是超可解的，所以G也是超可解的. 这就证明了定理.

第二十章　群论和射影平面

20.1. 公　　理

射影平面是指这样的点集，其中某些特选的子集叫做线，满足下列公理：

$P1$. 任何两个不同的点包含在唯一的一条线内.

$P2$. 任何两条不同的线包含唯一的一个公共点.

$P3$. 存在四个点，其中没有三个包含在一条线内.

包含两个不同的点 A 和 B 的唯一的线 k 叫做 A 和 B 的连线. 包含在两条不同的线 k 和 t 内的唯一的点 P 叫做 k 和 t 的交点.

设 A_1, A_2, A_3, A_4 是四个点，没有三个在一条线上，它们的存在由 $P3$ 决定. 那么就存在不同点对的六条不同的连线：

$$L_1:\ A_1A_2B_1.$$
$$L_2:\ A_1A_3B_2.$$
$$L_3:\ A_1A_4B_3.$$
$$L_4:\ A_2A_3B_3.$$
$$L_5:\ A_2A_4B_2.$$
$$L_6:\ A_3A_4B_1.$$

这里点 B_1, B_2, B_3 是这些线的交点，又由于这些线不同，容易证明这些 B 与 A 不同而且彼此不同.

引理 20.1.1. 每条线至少包含三个点：

证明. 上面构造出的线 $L_1\cdots$, L_6 中每一条至少包含三个点. 任何线 L，要是不包含 A_1，将与 L_1, L_2, L_3 相交于三

个不同的点．如果 L 不包含 A_2，则 L 与 L_1，L_4，L_5 相交于三个不同的点． 如果 L 同时包含 A_1 和 A_2，则 L 是 L_1，它至少包含三个点 A_1，A_2，B_1．

引理 20.1.2. 存在四条线，其中没有三条包含同一个点．

证明. 这里 L_1，L_2，L_5，L_6 就是没有三条相交于一个公共点的四条线．

如果我们交换点和线的地位而且把"包含"换成"包含在……内"，则公理 $P1$ 和 $P2$ 交换而且公理 $P3$ 和引理 20.1.2 交换．这就导出对偶这个概念．说得更清楚些，如果 π 是任何射影平面，则存在与 π 对偶的平面 π^*，它可以构造如下：

设 $\{P_i\}$ 是 π 的点集而且 $\{k_j\}$ 是 π 的线集．那么在 π^* 内存在与 π 的点 $\{P_i\}$ 成一一对应的线 $\{p_i\}$ 和与 π 的线 $\{k_j\}$ 成一一对应的点 $\{K_j\}$．其次，如果在 π 内 $P_i \in k_j$，则在 π^* 内令 $K_j \in p_i$，这里 $k_j \rightleftarrows K_j$ 和 $P_i \rightleftarrows p_i$．通过观察可以证明，如果 π 满足射影平面的公理，则 π^* 也是如此． 再有，π^* 的对偶是 π，即 $(\pi^*)^* = \pi$． 因此，交换点和线的地位而且改变包含关系以后，关于 π 的每一个表述变成关于它的对偶 π^* 的表述．这就是对偶原则．特别根据对偶原则，如果某个命题对于射影平面 π 成立，则这命题的对偶也成立．例如应用对偶原则，引理 20.1.1 变成：

引理 20.1.3. 每个点至少在三条线上．

读者不难验证，这里给的公理等价于射影几何中关于平面的公理，如同在韦勃伦和杨合著的《射影几何学》(Veblen and Young [1]) 第一卷第 16—18 页上所给的那样．

假定射影平面 π 的线 L_1 包含有限个点． 把点的个数记做 $n+1$，根据引理 20.1.1，$n \geqslant 2$． 根据公理 $P3$，至少存在两个点 P_3 和 P_4 不在 L_1 上． 设 P_3P_4 与 L_1 相交于 B_1，再设 P_1 和 P_2 是 L_1 的另外两个点． 那么 P_1P_3 和 P_2P_4 相交于既不在

L_1 上也不在 P_1P_2 上的点 B_2. 设 P 是不在 L_1 上的任意点，连结 P 与 L_1 的 $n+1$ 个点. 我们得出通过 P 的 $n+1$ 条线，这是全部通过 P 的线，因为通过 P 的每一条线必定与 L_1 相交. 特别说来存在着通过 P_3, P_2 和 B_2 中每一个的 $n+1$ 条线. 现在设通过点 P 有 $n+1$ 条线，这些线与不通过 P 的线 L 相交于 $n+1$ 个点，这些点是 L 上的全部点，因为 L 上的每个点都与 P 有连线. 因此 π 的每条线 L 包含 $n+1$ 个点. 因为 P_3, P_4 和 B_2 至少有一个不在 L 上. 又通过 π 的每个点 P 都有 $n+1$ 条线，它们是 P 与不通过 P 的某条线 L 上的 $n+1$ 个点的连线，我们证明了下列定理的主要部分.

定理 20.1.1. 设 $n \geqslant 2$ 是整数. 在射影平面上下列性质是等价的.

1) 一条线恰好包含 $n+1$ 个点.
2) 一个点恰好在 $n+1$ 条线上.
3) 每条线恰好包含 $n+1$ 个点.
4) 每个点恰好在 $n+1$ 条线上.
5) 在 π 上恰好存在 n^2+n+1 个点.
6) 在 π 上恰好存在 n^2+n+1 条线.

证明. 我们已经证明从 (1) 得出 (2), (3) 和 (4). 为了证明 (5), 设 P_0 是 π 的点而且 $L_1, \cdots, L_{n+1}$ 是通过 P_0 的 $n+1$ 条线. 这些线包含了 π 的全部点，而且每一条都包含 P_0 和另外 n 个点. P_0 是 $L_1, \cdots, L_{n+1}$ 中任何两条的唯一的公共点. 因此 π 包含 $1+(n+1)n = n^2+n+1$ 个点. 为了证明 (6), 设 L_0 是 π 的线而且 $P_1, \cdots, P_{n+1}$ 是 L_0 的 $n+1$ 个点. 每个点 $P_1, \cdots, P_{n+1}$ 在 L_0 和另外 n 条线上. 这样我们得出 π 的全部线，因而在 π 上有 $1+(n+1)n = n^2+n+1$ 条线. 因此从性质 (1) 得出所有其余的性质. 根据对偶性，从(2)也得出其余的性质. 显然从 (3) 得 (1), 从 (4) 得 (2).

如果 (5) 成立而且有某条线具有 $m+1$ 个点，这里 m 是整数，则 π 有 $m^2+m+1=n^2+n+1$ 个点，因而 $m=n$，即从 (5) 得 (1). 同理，从 (6) 得 (2).

20.2. 直射和德沙格定理[1)]

如果在平面 π_1 的点 $\{P_1\}$ 和平面 π_2 的点 $\{P_2\}$ 之间存在一一对应 $P_1 \rightleftarrows P_2=(P_1)\alpha$，而且在 π_1 的线 $\{k_1\}$ 和 π_2 的线 $\{k_2\}$ 之间存在一一对应 $k_1 \rightleftarrows k_2=(k_1)\beta$，使得在 $P_1 \in k_1$ 时有 $(P_1)\alpha \in (k_1)\beta$，则就说平面 π_1 同构于平面 π_2. 明显地，对应 α 和 β 中的每一个完全决定另一个，而且如果当 π_1 的三个点 P_1, Q_1 和 R_1 在一条线上时，$(P_1)\alpha$, $(Q_1)\alpha$ 和 $(R_1)\alpha$ 就在一条线上，则点的这样的一一对应 $P_1 \rightleftarrows (P_1)\alpha$ 就决定一个同构。同理，如果每三条共点的线对应于三条共点的线，则线的这样的一一对应就决定一个同构. 平面的同态是指点和线的保持关联关系的多一对应，但是对于平面说这里不是像对于其他对象那样有价值的概念.

平面 π 到自身的同构 α 叫做直射. 平面的直射组成一个群.

可以嵌入三维空间 E_3 的平面 π_1 总有很大一族直射. 设 π_2 是 E_3 中的另一个平面，又 L 是 π_2 与 π_1 的交线. 在 E_3 中取不在 π_1 或 π_2 上的任意两个点 P_1 和 P_2. 定义以 P_1 为中心的从 π_1 到 π_2 上的透视，这是从 π_1 的任意点 Q 到 π_2 的点 R 的映射，记做

$$Q \xrightarrow{P_1} R, \tag{20.2.1}$$

这里 R 是线 P_1Q 与 π_2 的交点. 这时 P_1QR 在一条线上，而且

---

1) 关于在这里用到的三维空间的性质，参看 Veblen and Young [1]，第 20—25 页.

$Q\in\pi_1$, $R\in\pi_2$. 透视 (20.2.1) 是从 π_1 到 π_2 上的同构，因为如果 M_1 是 π_1 的线，则包含 M_1 和 P_1 的平面与 π_2 相交于线 M_2，而且已知的透视把 M_1 的点映成 M_2 的点. 其次，L 的每个点都映成自己，因为 L 是 π_1 和 π_2 的交线，设在透视 (20.2.1) 之后再进行以 P_2 为中心把 π_2 映到 π_1 上的透视

$$R\xrightarrow{P_2}S, \tag{20.2.2}$$

这也是保留 L 的全体点不变的从 π_2 到 π_1 上的同构. 这样两个透视的联合.

$$Q\xrightarrow{P_1}R\xrightarrow{P_2}S \tag{20.2.3}$$

是保留 L 的全体点不变的 π_1 的直射. 再设 O 是线 P_1P_2 与 π_1 的交点. 我们将有

$$O\xrightarrow{P_1}T\xrightarrow{P_2}O, \tag{20.2.4}$$

因为 P_1P_2OT 在一条线上，因而 $(O)\alpha=O$. 其次设 k 是通过 O 的任意线. 如果 Q 是 k 的点，则(20.2.3)中的 R 将处在包含相交的线 k 和 P_1P_2OT 的平面 π_4 上，因而 (20.2.3) 中的 S 也是 π_4 的点，即也是 k 的点. 因此 α 把通过 O 的每条线变成自己. 这样的直射叫做透视直射，有时也叫做透视. 全体点在 α 下都不变的线 L 叫做直射的轴，通过它的每条线都不变的点 O 叫做直射的中心. 中心 O 可以在也可以不在轴 L 上，如果我们希望区分这两种情形，则把中心 O 在轴 L 上的直射叫做合射，而把中心 O 不在轴 L 上的直射叫做透射. 透视直射的性质可以从附于德沙格定理的图上看到.

假定 α 是具有中心 O 和轴 L 的透视直射，而且 A_1 是 π 的既不在 L 上也不是 O 的点. 那么 $(A_1)\alpha=A_2$ 必定在线 OA_1 上. 现在给了 O, L, A_1 和 A_2，这里 O, A_1, A_2 共线而且 A_1 和 A_2 既不在 L 上，也不是 O，我们来断定具有中心 O 和轴 L 而且使 $(A_1)\alpha=A_2$ 的直射 α 是完全确定的. 设 B_1 是 π 的不

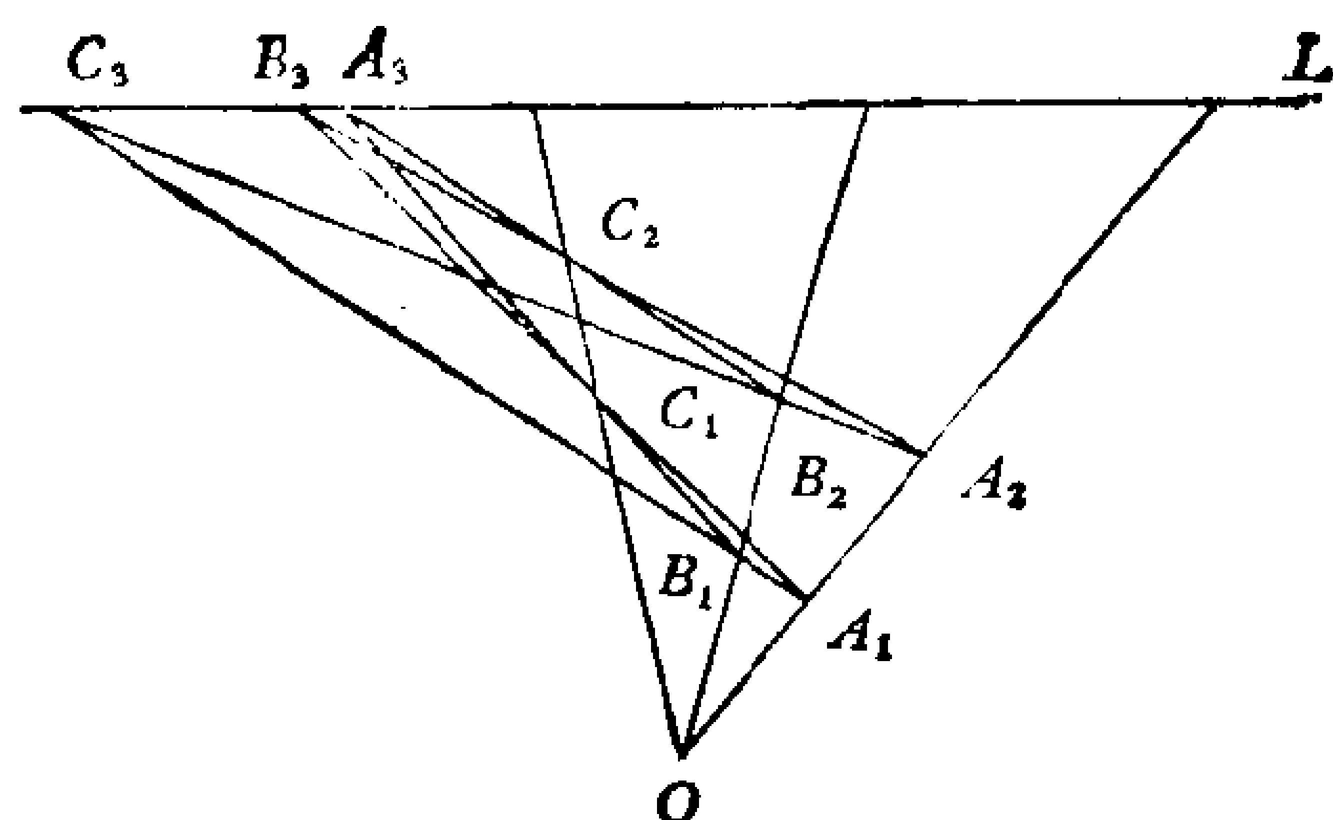


图 9 德沙格定理

在 OA_1A_2 或 L 上的点. 设 A_1B_1 与 L 相交于 C_3. 那么 $(B_1)\alpha$ 必定在 OB_1 上. 但是因为 A_1, B_1, C_3 共线,所以 $(A_1)\alpha=A_2$, $(B_1)\alpha$ 和 $(C_3)\alpha=C_3$ 也必定共线. 因此 $(B_1)\alpha$ 必定同时在 OB_1 和 C_3A_2 上,因而 $(B_1)\alpha=B_2$ 是 OB_1 和 C_3A_2 的交点. 因此,在已知 $(A_1)\alpha=A_2$ 时,不在 OA_1A_2 上的每个点 B_1 的像就完全决定了. 而在已知 $(B_1)\alpha=B_2$ 以后, OA_1A_2 上的点的像也就唯一决定了.

现在设 C_1 是不在 OA_1A_2 或 OB_1B_2 上的点. 再设 B_1C_1 与 L 相交于 A_3, A_1C_1 与 L 相交于 B_3. 那么 $(C_1)\alpha=C_2$ 就作为 A_2B_3 和 OC_1 的交点而决定. 但是因为 B_1, C_1, A_3 共线, 所以 $(B_1)\alpha=B_2$, $(C_1)\alpha=C_2$ 和 $(A_3)\alpha=A_3$ 也共线, 这就给出大家叫做德沙格巧图的一种图形. 这种巧图的存在叫做德沙格定理. 我们说三角形 $A_1B_1C_1$ 和 $A_2B_2C_2$ 以 O 为中心而成透视,假如对应的顶点在通过 O 的同一条线上,即 OA_1A_2, OB_1B_2 和 OC_1C_2 都是线. 又如果对应的边相交于 L 的点, 则说三角形以 L 为轴而成透视.

定理 20.2.1 (德沙格定理). 如果两个三角形 $A_1B_1C_1$ 和 $A_2B_2C_2$ 以 O 为中心而成透视, 则对应边 A_1B_1 和 A_2B_2, A_1C_1 和 A_2C_2, B_1C_1 和 B_2C_2 的交点 C_3, B_3, A_3 在一条线 L 上.

德沙格定理在平面 π 上成立等价于 π 上所有可能的透视

直射的存在，这从下列定理得出.

定理 20.2.2. 在平面 π 上给了线 L，点 O 和既不是 O 又不在 L 上的两个点 A_1，A_2，并且 O，A_1，A_2 共线. 那么最多存在 π 的一个透视直射 α 以 O 为中心而且以 L 为轴，并且 $(A_1)\alpha = A_2$. 如果 π 能嵌入三维空间，则这种直射存在.

证明. 我们在上面看到，给了中心 O，轴 L 而且 $(A_1)\alpha = A_2$，这里 O，A_1，A_2 共线，那么透视直射就完全决定. 因此最多存在 π 的一个这种直射. 现在假定 π 能嵌入三维空间 E_3. 在 E_3 中取与 π 相交于 L 的平面 π_2，而且取 E_3 的不在 π 和 π_2 上的点 P_1. 连结 P_1 与 O 而且设 P_1O 与 π_2 相交于 T（参看图 10）.

如果 A_1P_1 与 π_2 相交于 Q，则 Q 和 A_2 同在由 OP_1 和 OA_1A_2 决定的平面 π_3 上，π_3 就是图 10 所在的平面. 因此 A_2Q 与 OP_1 相交于点 P_2. 然而 P_2 不在 π_2 上，因为否则它就将是 T 因而 A_2 将与 OA_1A_2 和线 L 的交点 X 重合，这与 A_2 不在 L 上的假设矛盾. 同理，因为 A_2 不是 O，所以 P_2 不在 π 上. 现在我们看到透视直射 α

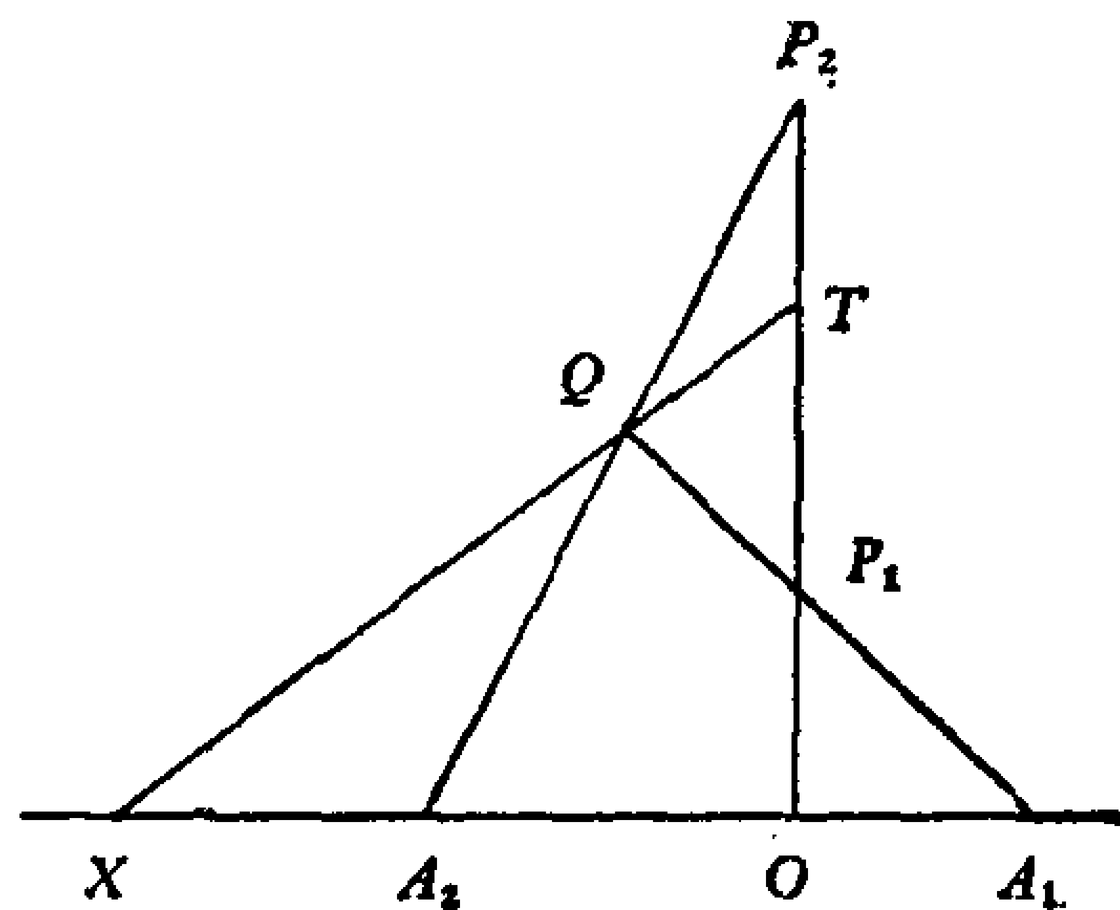


图 10 透视

$$\pi \xrightarrow{P_1} \pi_2 \xrightarrow{P_2} \pi$$

以 L 为轴和以 O 为中心；我们还有 $A_1 \xrightarrow{P_1} Q \xrightarrow{P_2} A_2$，因此，$A_2 = (A_1)\alpha$，这是我们所要求的，因而定理中的直射存在.

定理 20.2.3. 德沙格定理在平面 π 上成立，必要而且只要在 π 上存在所有可能的透视直射.

推论 20.2.1. 德沙格定理在可以嵌入三维射影空间的平

面 π 上成立.

证明. 只要证明了定理,就可以从前面一个定理得出上述推论.

先假定在平面 π 上存在所有可能的透视直射. 设给了两个三角形 $A_1B_1C_1$ 和 $A_2B_2C_2$ 使得三条线 A_1A_2, B_1B_2 和 C_1C_2 相交于点 O. (参看关于德沙格定理的图.) 设 A_1B_1 和 A_2B_2 相交于点 C_3, A_1C_1 和 A_2C_2 相交于点 B_3. 把 B_3 和 C_3 的连线记做 L. 那么根据假设, 存在以 O 为中心和以 L 为轴的透视直射 α, 使得$(A_1)\alpha = A_2$. 于是根据我们的作图,$(B_1)\alpha = B_2$ 和 $(C_1)\alpha = C_2$. 设 B_1C_1 与 L 相交于 A_3, 那么 $(B_1)\alpha = B_2$, $(C_1)\alpha = C_2$ 和 $(A_3)\alpha = A_3$ 共线, 因而 B_1C_1 和 B_2C_2 的交点 A_3 与 B_3 和 C_3 共线. 这就证明了德沙格定理.

反之, 假定德沙格定理在平面 π 上成立. 设给了线 L 和不共线的点 O, A_1, A_2, 而且 A_1 和 A_2 都不在 L 上 (但是 O 可以在 L 上). 我们定义 π 的点的映射 α, 来证明它是直射. (我们仍然参看关于德沙格定理的图.) 对于 L 上的任何点 X, 令 $(X)\alpha = X$. 又令 $(O)\alpha = O$ 以及$(A_1)\alpha = A_2$. 如果 B_1 既不在 L 上也不在 OA_1A_2 上, 设 A_1B_1 与 L 相交于 C_3, 如果 A_2C_3 与 OB_1 相交于 B_2, 令 $(B_1)\alpha = B_2$. 这对于除 OA_1A_2 上的点外的 π 的全体点定义了映射 α. 现在如果 A_1C_1 与 L 相交于 B_3, 则当 A_2A_3 与 OC_1 相交于 C_2 时, 我们令 $C_2 = (C_1)\alpha$. 如果 OA_1, OB_1 和 OC_1 是不同的线, 则三角形 $A_1B_1C_1$ 和 $A_2B_2C_2$ 以 O 为中心而成透射, 因而根据德沙格定理, 对应边的交点共线. 但是 C_3 和 B_3在 L 上, 因而 B_1C_1 和 B_2C_2 相交于 L 上的 A_3. 但是要是我们从 $(B_1)\beta = B_2$ 开始. 我们可以把 $(C_1)\beta$ 定义为 B_2A_3 和 OC_1 的交点. 而这个交点是 C_2, 因此我们有 $(C_1)\alpha = (C_1)\beta = C_2$ 同时作为 $(A_1)\alpha = A_2$ 和 $(B_1)\beta = B_2$ 的结果. 因而映射 $\alpha = \beta$ 在它们都有定义的所有的线 (例如

OC_1C_2) 上相合. 但是 α 在整个 OB_1B_2 上有定义, β 在整个 OA_1A_2 上有定义. 因此映射 α 对于 π 的全体点都有定义.

再根据 $(A_1)\alpha = A_2$ 而且 k 是不通过 O 或 A_1 的任意线的同一个图,设 k 与 L 相交于 A_3 而且 B_1 和 C_1 是 k 上的另两个点. 那么根据定义, $(B_1)\alpha = B_2$, $(C_1)\alpha = C_2$ 和 $(A_3)\alpha = A_3$, 因而把德沙格定理应用到三角形 $A_1B_1C_1$ 和 $A_2B_2C_2$, 就能得出 B_2, C_2 和 A_3 共线. 这说明映射 α 把 $k = A_3B_1$ 的点 C_1 变成 A_3,B_2 的点, 除非 C_1 是 A_3B_1 与 OA_1A_2 的交点. 但是当 $C_1 = D_1$ 是 B_1A_3 与 OA_1A_2 的交点时,根据 $(B_1)\alpha = (B_1)\beta = B_2$, 可以定义 $(D_1)\beta = D_2$ 为 A_3B_2 与 OA_1A_2 的交点 D_2. 因此这映射把 k 的全部点变成 A_3B_2 的点. 明显地,这映射把 L 变成自己而且把通过 O 的线变成自己. 因此 α 是所要的直射.

我们实际上已经证明了比定理 20.2.3 更详尽的结果. 我们把它写成一个定理.

定理 20.2.4. 在平面 π 上存在具有已知中心 O 和已知轴 L 的所有可能的直射, 必要而且只要德沙格定理对于所有以 O 为中心而成透射的三角形都成立, 即当他们有两对对应边相交于 L 上时,第三对对应边也相交于 L 上.

并非每个平面 π 都能嵌入三维空间,而且存在定理 20.2.4 只对少数几个轴 L 和中心 O 成立的情形.

20.3. 坐标的导人

设在任意射影平面 π 上取四个点 X, Y, O, I, 没有三个共线. 把线 XY 叫做无穷远线 L_∞. 把线 OI 叫做 $x = y$ 线.

在线 OI 上令 O 的坐标为 (0, 0), I 的坐标为 (1, 1), 又令 OI 和 XY 的交点 C 有单独的坐标 (1). 对于 OI 的其他的点给以坐标 (b, b),不同的点取不同的记号 b. 对于不在 L

上的点 P，设 XP 与 OI 相交于 (b, b)，YP 与 OI 相交于 (a, a). 那么令 P 的坐标为 (a, b). 这个规则重新给 OI 的点以同样的坐标. 设连结 $(0, 0)$ 和 $(1, m)$ 的线与 L 相交于点 M. 给 M 以单独的坐标 (m)，这我们可以直观地设想为斜率. 这样我们就使 Y 以外的每个点都具有了坐标，对于 Y 我们给以单个的记号 (∞) 作为坐标.

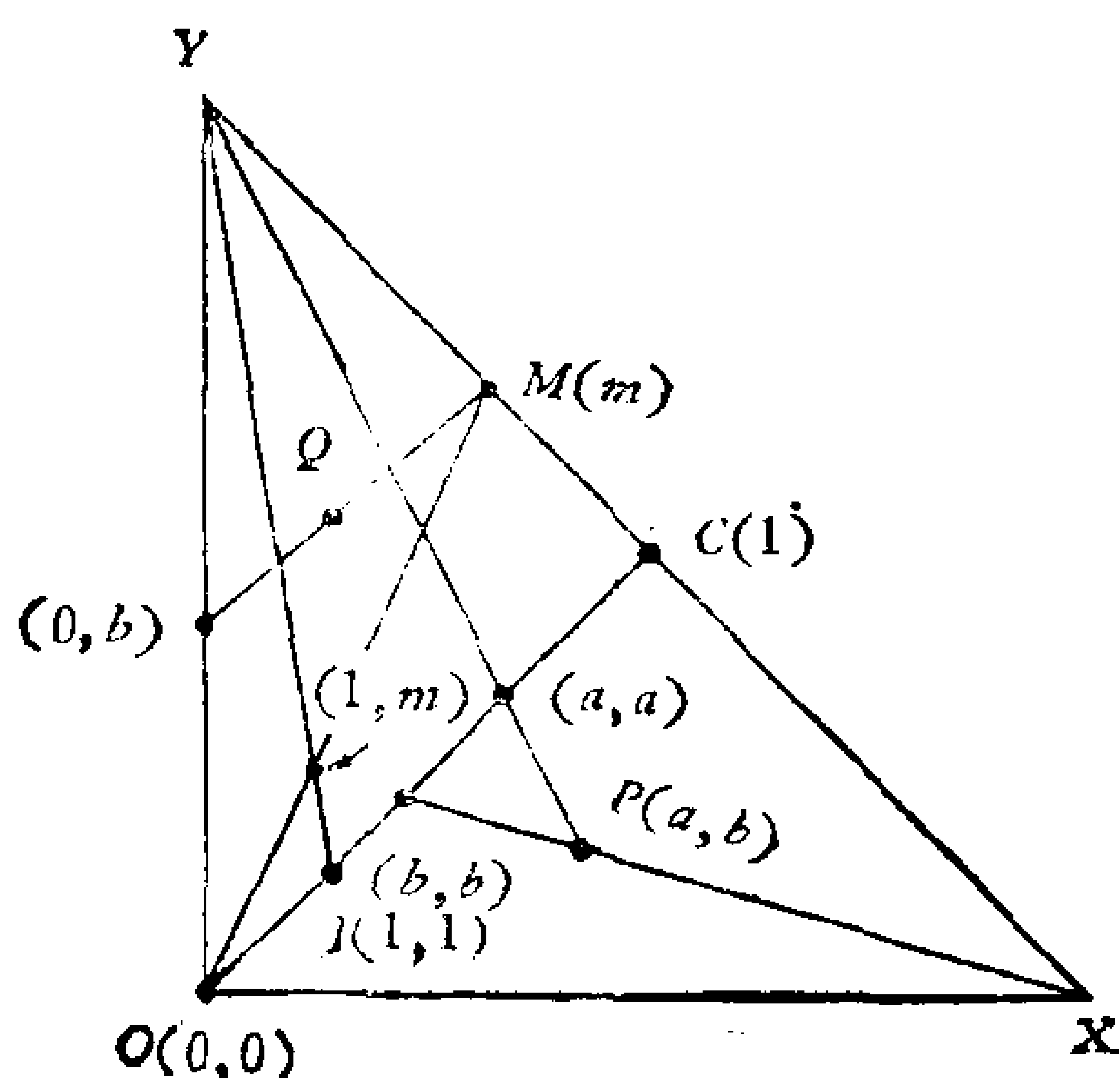


图 11　坐标的导入

我们利用平面上的线来定义坐标系上的代数运算. 这个代数体系是三元环，而且 π 上除 L_∞ 外的每条线都将有以三元环的运算表出的方程. 如果 (x, y) 是 OI 的有限点，我们有 $y = x$，因而我们取 $y = x$ 作为 OI 的方程. 通过 Y 而且不是 L_∞ 的线具有性质：它的全体有限点 (x, y) 都有相同的 x 坐标 $x = c$，因而可以把它取作线的方程.

如果 (x, y) 是 $C = (1)$ 和 $(0, b)$ 的连线上的有限点，我们用

$$y = x + b \tag{20.3.1}$$

定义一个二元加法运算，而且取它作为这线的方程. 如果 (x, y) 是 $O = (0, 0)$ 和 (m) 的连线上的有限点，我们用

$$y = xm \tag{20.3.2}$$

定义一个二元乘法运算，而且取它作为这条线的方程．一般地，不通过 Y 的任何线与 L_∞ 相交于某个点 (m) 并且与 OY 相交于某个点 $(0, 6)$．如果 $Q = (x, y)$ 是这条线的点，我们定义一个三元运算

$$y = x \cdot m \circ b, \tag{20.3.3}$$

而且取它作为这条线的方程．因而加法和乘法都是这个三元运算的特例．即我们有

$$\begin{aligned} x + b &= x \cdot 1 \circ b, \\ xm &= x \cdot m \circ 0. \end{aligned} \tag{20.3.4}$$

元素 0 和 1 具有熟知的性质

$$\begin{aligned} 0 + a = a + 0 &= a, \\ 0m = m0 &= 0. \\ 1m = m1 &= m. \end{aligned} \tag{20.3.5}$$

平面 π 可以表成一个三元环 R，它的三元运算满足某些性质，而且反之，具有这些性质的三元环唯一决定一个平面．我们把这写成关于三元环的主要定理．

定理 20.3.1. 在平面 π 上选取没有三点共线的四个点 X, Y, O, I，就决定一个三元环 R. R 的元素包括一个零 0 和一个单位元素 $1 \neq 0$．三元运算 $x \cdot m \circ b$ 满足下列定律:

$T1$. $0 \cdot m \circ c = a \cdot 0 \circ c = c$.

$T2$. $1 \cdot m \circ 0 = m \cdot 1 \circ 0 = m$.

$T3$. 给定 a, m, c，恰好存在一个 z，使得 $a \cdot m \circ z = c$.

$T4$. 给定 $m_1 \neq m_2$, b_1, b_2，就存在唯一的 x，使得

$$x \cdot m_1 \circ b_1 = x \cdot m_2 \circ b_2.$$

$T5$. 给定 $a_1 \neq a_2$, c_1, c_2，就存在唯一的一对 m, b，使得

$$a_1 \cdot m \circ b = c_1 \text{ 和 } a_2 \cdot m \circ b = c_2$$

证明. 在平面 π 上取定没有三个在一条线上的四个点

X, Y, O, I，我们像上面那样构造一个具有运算 $x \cdot m \circ b$ 的三元环．性质 $T1$ 和 $T2$ 是定义的直接结果．$T3$ 是说 (m) 和 (a, c) 的连线与 OY 相交于唯一的点 $(0, z)$．$T4$ 是说具有不同斜率 m_1 和 m_2 的两条线 $y = x \cdot m_1 \circ b_1$ 和 $y = x \cdot m_2 \circ b_2$ 相交于唯一的有限点．$T5$ 是说如果 (a_1, c_1) 和 (a_2, c_2) 是 $a_1 \neq a_2$ 的两个有限点，则就存在唯一的线 $y = x \cdot m \circ b$ 通过这两个点．

反之，假定给了一个三元环 R 满足 $T1, \cdots, T5$．我们构造有限点 (a, b) 和无穷点 (m) 和 (∞)，这里 a, b, m 遍历 R 的元素．线 L_∞ 包含全体无穷点 m，(∞) 而不包含别的．具有固定的 c 的全体点 (c, y) 以及 (∞) 是一条线 $x = c$ 的点．对于固定的 m 和 b，点 (m) 和使 $y = x \cdot m \circ b$ 的点 (x, y) 是一条线 $y = x \cdot m \circ b$ 的点．需要考虑好多情形，但是容易得出上述公理的自然结果是：两个不同的点在唯一的一条线上，两条不同的线相交于唯一的点，又四个点 (∞)，(0)，$(0, 0)$ 和 $(1, 1)$ 没有三个共线．我们只验证一点，其他的是相仿的．考虑两条不同的线 $y = x \cdot m_1 \circ b_1$ 和 $y = x \cdot m_2 \circ b_2$．它们有公共的无穷点 (m)，而没有别的公共无穷点．如果它们还有公共的有限点 (a, c)，则就有 $a \cdot m \circ b_1 = c = a \cdot m \circ b_2$，这将与 $T3$ 矛盾，因为 $b_1 \neq b_2$．

20.4. 韦勃伦-魏德本体系．赫尔体系

我们要来研究具有某些直射群的平面的性质，而且把这些性质与建立坐标的三元环连系起来．

引理 20.4.1. 射影平面 π 上不变两条不同的线上的每个点的直射是恒同直射．

证明． 设直射 α 不变线 L_1 和 L_2 上的每个点而且 L_1 和

L_2相交于点 Q，设 P 是 π 的不在 L_1 和 L_2 上的任意点．取 L_1 上不是 Q 的两个点 R 和 S．设 PR 与 L_2 相交于 T，PS 与 L_2 相交于 U，那么 R，S，T，U 在 α 下不变，因而线 RT 和 SU 在 α 下也不变，因此它们的交点 P 也不变．总之，不仅 L_1 和 L_2 的点在 α 下不变，而且不在 L_1 和 L_2 上的每个点 P 在 α 下也不变，因而平面 π 的每个点都不变，所以 α 是恒同直射．

引理 20.4.2. 射影平面上不变一条线上的每个点和不在这线上的两个点的直射是恒同直射．

证明． 设直射 α 不变线 L 上的每个点和不在 L 上的两个点 P_1 和 P_2，设 P 是平面上既不在 L 上也不在线 P_1P_2 上的任意点．设 P_1P 与 L 相交于 Q_1，P_2P 与 L 相交于 Q_2，因为 P 不在 P_1P_2 和 L 上，线 P_1PQ 和 P_2PQ_2 不同．因为 P_1，Q_1，P_2，Q_2 是不同的不变点，线 P_1Q_1 和 P_2Q_2 是 α 的不变线，因而它们的交点 P 不变．因此 α 不变 L 上的每个点和不在 P_1P_2 上的每个点．因此 α 不变 L 上和通过 P_1 而不是 P_1P_2 的某条线（例如 P_1Q_1）上的每个点．因此根据引理 20.4.1，α 是恒同直射．

总之我们发现，非恒同的直射如果不变一条线上的每个点，最多只能不变不在这线上的一个点．

定理 20.4.1 给了平面上不变一条线 L 和 L 上的每个点的直射 α．那么就存在点 C，使得 α 不变 C 和通过 C 的每一条线．如果 α 不是恒同，则 α 没有其它不变的点和线．作为对偶，如果 α 不变一个点 C 和通过 C 的每一条线，则存在线 L，使得 α 不变 L 和 L 上的每个点，而且如果 α 不是恒同，则它没有其它的不变点和线．

证明． 设 $\alpha \neq 1$ 是平面 π 的不变线 L 上每个点的直射，那么根据引理 20.4.2，α 最多还不变不在 L 上的一个点．先

假定 α 不变不在 L 上的点 C. 那么通过 C 的一条线与 L 相交于不是 C 的点 Q, 而且因为 C 和 Q 都在 α 下不变,所以线 CQ 在 α 下不变, 因而通过 C 的每条线在 α 下都不变. 如果除 L 和通过 C 的线外还有一条不变的线 L_2, 则 L_2 上作为 L_2 与通过 C 的线的交点的每一个点都不变, 因而根据引理 20.4.1, α 是恒同. 同理,根据引理 20.4.2, 不可能有在 α 下不变的其它的点.

现在假定 α 没有不在 L 上的不变点. 设 P 是不在 L 上的点. 那么 P 在 α 下的像 $P\alpha$ 与 P 不同而且不在 L 上. 因此线 $M = PP_\alpha$ 与 L 相交于点 $C \neq P$ 和 P_α. 因而 $M = PC$ 和 $M\alpha = P\alpha C\alpha = P\alpha C$. 但是 P, $P\alpha$, C 共线,因而 $M = M\alpha$. 因此不在 L 上的每个点 P 在一条不变的线 M 上. 其次, 这样的 P 不可能在两条不同的不变线上, 因为这时它本身就要不变了. 现在设 $M = PC$ 是一条不变的线, 考虑既不在 L 上又不在 M 上的点 Q.那么 Q 也在唯一的不变线 N 上.现在 M 和 N 的交点是不变点, 而根据假设不存在不在 L 上的不变点. 因此 N 与 M 相交于 L 上的点 C. 于是每条不变线都通过 C. 而通过 C 的不是 L 的任意线总包含不在 L 上的点 R. R 也在通过 C 的一条不变的线上,因而这条不变的线必须是 $RC = K$. 因此通过 C 的每条线是不变的线. 这时如果除 L 和它的点以及 C 和通过它的线以外, 还有其它不变的元素, 则根据引理 20.4.1 和 20.4.2, α 仍将是恒同.

定理的其余部分根据对偶性得出.

因此定理里的直射正是在 § 20.2 里讨论过的透视直射. 这些直射有时叫做**中心直射**. 当我们想要突出中心 C 和轴 L 时,我们说它是 C–L **直射**. 具有中心 C 和轴 L 的全体直射显然组成一个群. 在 § 20.2 中我们把中心 C 在轴 L 上的直射叫做**合射**, 而把 C 不在 L 上的直射叫做**透射**.

引理 20.4.3. 中心直射 α 由中心 C，轴 L 和不在 L 上的任何不是 C 的点 P 的映射 $P \to P\alpha$ 完全决定. $P, P\alpha$ 和 C 必定共线.

证明. 如果存在两个具有中心 C 和轴 L 的直射 α_1 和 α_2，而且 $P\alpha_1 = P\alpha_2$，那么 $\alpha_1\alpha_2^{-1}$ 不变 L 的点，并具有中心 C 而且不变 P. 于是根据定理 20.4.1，$\alpha_1\alpha_2^{-1} = 1$，即 $\alpha_1 = \alpha_2$. 这就是引理所断定的.

定理 20.4.2. 具有相同的轴 L 和不同的中心 C_1 和 C_2 的两个合射的乘积是具有轴 L 和中心 $C_3 \neq C_1$ 和 C_2 的合射.

证明. 设 α_1 是具有中心 C_1 在轴 L 上的合射，α_2 是具有中心 $C_2 \neq C_1$ 在轴 L 上的合射. 那么 $\alpha_1\alpha_2$ 是不变 L 的全体点的直射. 因此根据定理 20.4.1，$\alpha_1\alpha_2 = \alpha_3$ 是具有轴 L 的中心直射. 为了证明 α_3 是合射，我们必须证明 α_3 没有不在 L 上的不变点. 如果 $P\alpha_3 = P$，则 $P\alpha_1 = P\alpha_2^{-1}$. 这时 $C_1, P, P\alpha_1$ 共线而且 $C_2, P, P\alpha_2^{-1}$ 共线. 因此如果 $P\alpha_1 = P\alpha_2^{-1}$，这两条线就要重合，因而它们与 L 的交点重合，这给出 $C_1 = C_2$ 而与假设矛盾. 因此 $\alpha_3 = \alpha_1\alpha_2$ 没有不在 L 上的不变点，因此它是具有中心 C_3 在 L 上的合射. 如果 $C_3 = C_1$，则 $\alpha_2 = \alpha_1^{-1}\alpha_3$ 是具有中心 C_1 的合射而与假设矛盾. 因此 $C_3 \neq C_1$，同理 $C_3 \neq C_2$.

我们考虑全体 C-L 直射的群 $G = G(C, L)$. 如果 $P \neq C$ 而且 $P \notin L$，则对于任何 $\alpha \in G$，$C, P, P\alpha$ 共线. 如果对于 CP 上的每个点 Q，$Q \neq C$，$Q \notin L$，存在 $\alpha \in G$ 使得 $P\alpha = Q$，则我们说 π 是 C-L 传递的. 这是说每个可能的 C-L 直射确实存在. π 是 C-L 传递的这句话，相当于对于通过 C 的线 M，$M \neq L$，C-L 直射传递地变换除 C 和 M 与 L 的交点以外的、M 的点. 这对于通过 C 的任意线 $M \neq L$ 都成立.

根据定理 20.4.2，具有轴 L 的全体合射组成一个群 $G(L)$. 我们把这个群 $G(L)$ 叫做具有轴 L 的平移群.

定理 20.4.3（白尔）[1]．如果对于轴 L 上的两个不同的中心 C_1 和 C_2，合射群 $G(C_1, L)$ 和 $G(C_2, L)$ 都不是单位元素群，则整个平移群 $G(L)$ 是阿贝尔群．又 $G(L)$ 的每个 $\neq 1$ 的元素或是 (1) 无限阶的，或是 (2) 同一素数 p 阶的．

证明． 假定 $\alpha_1(\neq 1) \in G(C_1, L)$ 和 $\alpha_2(\neq 1) \in G(C_2, L)$．设 P 是不在 L 上的任意点．那么我们有以下的线：

$L_1: C_1, P, P\alpha_1$; $L_2: C_2, P, P\alpha_2$.

$L_1\alpha_2: C_1, P\alpha_2, P(\alpha_1\alpha_2)$; $L_2\alpha_1: C_2, P\alpha_1, P(\alpha_2\alpha_1)$.

但是 C_2，$P\alpha_1$ 和 $(P\alpha_1)\alpha_2 = P(\alpha_1\alpha_2)$ 共线，而且 C_1，$P\alpha_2$ 和 $(P\alpha_2)\alpha_1 = P(\alpha_2\alpha_1)$ 共线．因此不同的线 $C_2P\alpha_1$ 和 $C_1P\alpha_2$ 的交点是 $P(\alpha_1\alpha_2)$，也是 $P(\alpha_2\alpha_1)$． 因此 $P(\alpha_1\alpha_2) = P(\alpha_2\alpha_1)$ 对于每个 $P \notin L$．因此 $\alpha_1\alpha_2 = \alpha_2\alpha_1$．因此当 $C_1 \neq C_2$ 时，元素 $\alpha_1 \in G(C_1, L)$ 与任何 $G(C_2, L)$ 的每个元素 α_2 可交换． 假定 $\beta_1 \neq 1$ 是 $G(C_1, L)$ 的另一个元素．那么 $\beta_1\alpha_2$ 是具有中心 $C_3 \neq C_1, C_2$ 的合射．因此 α_1 与 $\beta_1\alpha_2$ 可交换，而且因为 α_1 与 α_2 可交换，所以 α_1 与 β_1 也可交换．因此 $G(C_1, L)$ 的元素 $\alpha_1 \neq 1$ 与 $G(L)$ 的每个元素都可交换，所以 $G(L)$ 是阿贝尔群． 存在这样的例子，当具有 $C_i \in L$，$C_i \neq C_1$ 的每个其它的 $G(C_i, L) = 1$ 时，$G(C_1, L)$ 可以不是阿贝尔群．

如果 $G(L)$ 的每个元素都是无限阶的，则 (1) 成立． 如果 $G(L)$ 包含有限阶元素，则就存在素数阶元素 $\alpha_1 \in G(C_1, L)$，$\alpha_1^p = 1$． 于是对于 $\alpha_2 \neq 1 \in G(C_2, L)$，$C_2 \neq C_1$，我们有 $\alpha_1\alpha_2 = \alpha_3 \in G(C_3, L)$，$C_3 \neq C_1$ 和 C_2． 这时 $(\alpha_1\alpha_2)^p = \alpha_2^p = \alpha_3^p$ 是 $G(C_2, L)$ 和 $G(C_3, L)$ 的公共元素，因而是单位元素． 因此 $\alpha_2^p = 1$． 同理，从 $\alpha_2^p = 1$ 得出 $\beta_1^p = 1$ 对于任何 $\beta_1 \in G(C_1, L)$，因此 $G(L)$ 的除单位元素外的每个元素的阶都是 p．

1) 参看 Bear [10]．

定理 20.4.4. 如果平面 π 对于 L 上的两个中心 $C_1 \neq C_2$ 是 C_1-L 传递的和 C_2-L 传递的，则 π 对于每个 $C \in L$ 是 C-L 传递的.

证明. 取通过 $C \neq C_1, C_2$ 的线 $M \neq L$，而且设 P 和 Q 是 M 上的不同于 C 的任意两个点. 设 PC_1 和 QC_2 相交于 S. 再设 $\alpha_1 \in G(C_1, L)$ 使 $P\alpha_1 = S$ 和 $\alpha_2 \in G(C_2, L)$ 使 $S\alpha_2 = Q$. 根据 C_1-L 和 C_2-L 传递性，α_1 和 α_2 存在. 于是 $\alpha_1\alpha_2 = \alpha_3$ 是具有轴 L 的合射，而且 P, $P\alpha_3 = Q$ 和 C 共线. 因此 $\alpha_3 \in G(C, L)$，所以 π 是 C-L 传递的.

推论 20.4.1. 如果 π 是 C_1-L 传递的和 C_2-L 传递的，这里 $C_1 \neq C_2$ 是 L 的点，则 $G(L)$ 包含以 L 的点为中心的每个可能的合射. 如果 π 对于每个 $C \in L$ 都是 C-L 传递的，我们说 π 是相对于轴 L 的平移平面.

用使 π 具有坐标的三元环的性质说来，合射的意义是什么? 我们先考虑当 π 对于 L 上的点 C 是 C-L 传递的情形. 我们取轴 L 作为 L_∞，而且取中心作为 $Y = (\infty)$.

定理 20.4.5. 平面是 Y-L_∞ 传递的，必要而且只要在对应的坐标三元环 R 内有

1） $a \cdot m \circ b = am + b$，和

2） 加法是群运算

证明. 假定 π 是 Y-L_∞ 传递的，在图上取 YQV 作为 $x = 0$，$V = (0, 0)$，$Q = (0, b)$，$X = (0)$，$T = (1)$，$M = (m)$. 于是 MQ 是 $y = x \cdot m \circ b$. 在 MQ 上取 P 为 $P = (a, a \cdot m \circ b)$. 画出 VM，它是 $y = xm$，和 TQ，它是 $y = x + b$，以及 YP，它是 $x = a$. 于是 YP 和 VM 的交点 U 是 $U = (a, am)$. 然后画出 UX，它是 $y = am$. UX 和 VT（它是 $y = x$）相交于 $W = (am, am)$. 于是 YW（它是 $x = am$）与 QT（它是 $y = x + b$）相交于 $R = (am, am + b)$. 现在如

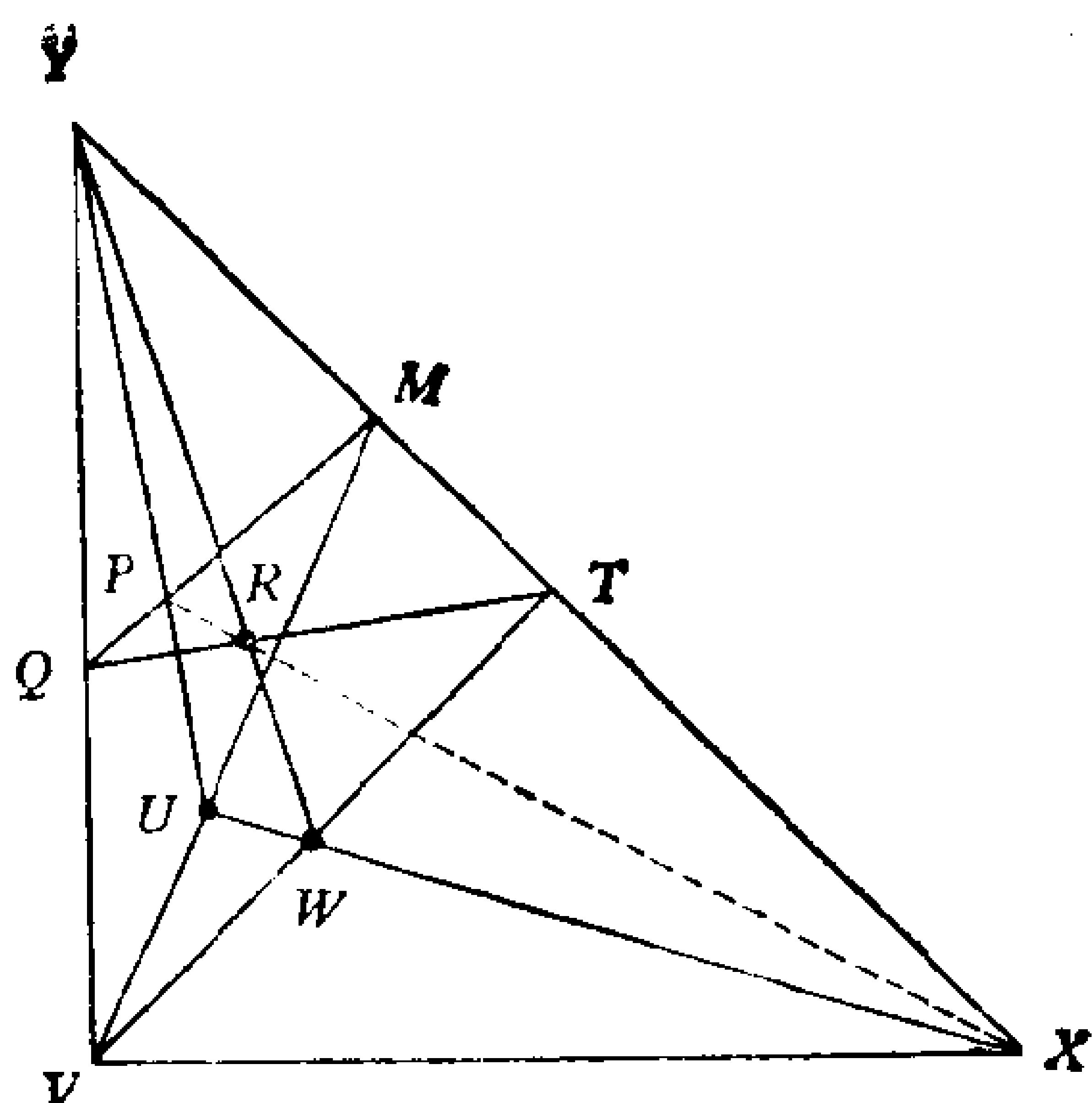


图 12 线性定理

果 P, R, X 共线，则因为 RX 是 $y = am + b$，我们根据 $P = (a, a \cdot m \circ b)$ 得出 $a \cdot m \circ b = am + b$. 因此我们需要证明 P, R, X 共线. 但是根据假设，π 是 $Y\text{-}L_\infty$ 传递的. 设 β 是不变 L_∞ 上的全体点和通过 Y 的全体线的直射，而且在通过 Y 的线 $x = 0$ 上，$V\beta = Q$ 即 $(0, 0)\beta = (0, b)$. 那么 β 不变线 YPU $(x = a)$ 和 $YRW(x = am)$. 其次，$(VM)\beta = QM$，$(VT)\beta = QT$. 因此 $U\beta = P, W\beta = R$，而且当然有 $X\beta = X$. 但是 U, W, X 在线 $y = am$ 上. 因此 $U\beta, W\beta, X\beta$ 即 P, R, X 在线 $y = xm + b$ 上. 因此 P 是 $(a, am + b)$ 而且 $a \cdot m \circ b = am + b$，定理的第一部分证明了.

由 $(0, 0)\beta = (0, b)$ 决定的直射 β 对一般的点 (a, c) 的作用如何？这易于用少数几步得出. 由于

$$y = x \to y = x + b,$$

$$x = c \to x = c$$

$$(c, c) \to (c, c + b),$$

$$y = c \to y = c + b$$

$$x = a \to x = a$$

$$(a, c) \to (a, c + b)$$

因此如果$(0,0)\beta = (0, b)$，则

$$(a, c)\beta = (a, c + b)$$

于是如果 δ 是由

$$(0, 0)\delta = (0, d)$$

决定的 Y-L_∞ 直射，则一般地有 $(u, v)\delta = (u, v + d)$.

对于 $\beta\delta$ 有

$$(0, 0)\beta\delta = [(0, 0)\beta]\delta = (0, b)\delta = (0, b + d).$$

因此一般地，$(a, c)\beta\delta = [a, c+(b + d)]$. 但是$[(a, c)\beta]\delta = (a, c + b)\delta = [a, (c + b) + d]$，因此加法满足结合律

$$c + (b + d) = (c + b) + d$$

因为平面上的加法总有零而且是络运算，所以加法是群运算. 因此我们证明了 (2).

反之，假定 π 的三元环 R 满足

1) $a \cdot m \circ b = am + b$，和

2) 加法是群运算.

对于任何 $b \in R$，定义映射 $\beta = \beta(b)$，使得对于点有：

$$(\infty) \to (\infty),$$
$$(m) \to (m),$$
$$(a, c) \to (a, c + b).$$

对于线有：

$$L_\infty \to L_\infty,$$
$$x = a \to x = a,$$
$$y = xm + t \to y = xm + (t + b).$$

这是直射，因为如果 (a, c) 在 $y = xm + t$ 上，则 $c = am+t$，因而

$$c + b = (am + t) + b = am + (t + b),$$

所以 $(a, c+b)$ 在 $y = xm + (t+b)$ 上. 为证明 β 是直射所需要的其他验算是容易的. 而这还是把 $(0, 0)$ 变成 $(0, b)$ 的 $Y\text{-}L_\infty$ 直射,又因为 b 是任意的,所以 π 是 $Y\text{-}L_\infty$ 传递的.

下面是关于直移平面的对应的定理:

定理 20.4.6. 平面 π 是相对于轴 L_∞ 的平移平面, 必要而且只要对应的三元环是韦勃伦-魏德本体系,这是说

1) 在加法下是阿贝尔群.

2) 在乘法下(不包括 0)是络.

3) $(a+b)m = am + bm$.

4) 如果 $r \neq s$, 则 $xr = xs + t$ 有唯一的解 x.

5) $a \cdot m \circ b = am + b$.

证明. 根据定理 20.4.4, 如果 π 既是 $Y\text{-}L_\infty$ 传递的又是 $X\text{-}L_\infty$ 传递的, 则它是具有轴 L_∞ 的平移平面, 从定理 20.4.5 可以得出 (5) 而且 R 在加法下是群. 在定理 20.4.5 的证明中, 我们指出了对于每个 $b \in R$, 存在合射 $\beta(b)$, 它把任意 (a, c) 映成 $(a, c+b)$, 根据定理 20.4.3, 整个平移群是阿贝尔群,因而

$$\beta(b)\beta(d) = \beta(d)\beta(b).$$

所以 $(a, c+b+d) = (a, c+d+b)$, 因而 $b+d = d+b$, 于是 R 内的加法是可交换的, 即证明了 (1).

设 b 是 R 的任意元素, 来考虑以 X 为中心而且把 $(0, 0)$ 变成 $(b, 0)$ 的合射. 我们依次有

$$(0, 0) \to (b, 0),$$

$$y = x \to y = x - b,$$

$$y = a \to y = a,$$

$$(a, a) \to (a+b, a),$$

$$x = a \to x = a + b,$$

$$y = am \to y = am,$$

$$(a, am) \to (a + b, am).$$

再因为 $(0, 0) \to (b, 0)$，所以

$$y = xm \to y = xm - bm.$$

然后因为 (a, am) 在 $y = xm$ 上，所以 $(a + b, am)$ 在 $y = xm - bm$ 上，因而

$$am = (a + b)m - bm,$$

所以 $am + bm = (a + b)m$. 这证明了分配律(3).

平面在乘法下总是络，而条件(4)是说当 $r \neq s$ 时，线 $y = xr$ 和 $y = xs + t$ 相交于唯一的有限点.

具有满足条件(1),(2),(3),(4)的加法和乘法运算的元素体系叫做韦勃伦-魏德本体系，因为这最先是在这两人的论文 (Veblen and Wedderburn [1]) 里提出的.

反之，我们来证明，任何韦勃伦-魏德本体系 R 可以用作具有轴 L_∞ 的直移平面的坐标系. 我们取作点的是: (1) 有限点 (a, b)，这里 a, b 是 R 的任意元素; (2) 无限点 (m)，这里 $m \in R$; (3)点 $Y = (\infty)$. 取作线的是: (1) 具有点 (∞) 和 (m) 的线 L_∞; (2) 包含 (∞) 和全体点 (c, d) 的线 $x = c$; (3) 包含点 (m) 和对于每个 $a \in R$ 的点 $(a, am + k)$ 的线 $y = xm + b$. 现在需要直接验证: 存在唯一的线连结两个不同的点，存在唯一的点在两条不同的线上，而且四个点 $(0, 0)$、$(1, 1)$, (∞) 和 (0) 中没有三个共线. 这种验算需要考虑几种情形，而且我们要用到条件(4)来证明当 $r \neq s$ 时线 $y = xr + b$ 和 $y = xs + c$ 相交于唯一的有限点.

对于韦勃伦-魏德本平面，我们易于验证有限点的映射 $(x, y) \to (x + r, y + s)$ 对于任何 r 和 s 都是直射，它不变 L_∞ 上的全体点而且对于有限线有 $x = c \to x = r + c$, $y = xm + b \to y = xm - rm + s + b$. 如果 $s = rt$，则这个直射是具有轴 L_∞ 和中心 (t) 的合射. 因此韦勃伦-魏德本平面是

具有轴 L_∞ 的直移平面.

当然，任何可结合的可除环是韦勃伦-魏德本体系，甚至任何非结合的可除环也是如此. 乘法可结合的韦勃伦-魏德本体系叫做准域. 这将在以后讨论. 值得注意而且将在以后说明(在 § 20.9 里)的是，非同构的韦勃伦-魏德本体系可以成为同一个平面的坐标系. 因为如果我们对于平移平面 π 改变线 L_∞ 上的点 X 和 Y 的选取，则根据定理 20.4.6，坐标三元环是韦勃伦-魏德本体系，但是并非这种体系都是同构的.

易于构造称为赫尔体系[1]的一类韦勃伦-魏德本体系. 假定在域 F 上存在不可约的二次多项式 $x^2 - rx - s$，则我们可以构造 F 上的韦勃伦-魏德本体系 J.

定理 20.4.7. 给了域 F 和 F 上不可约的二次多项式

$$f(x) = x^2 - rx - s.$$

那么 $a, b \in F$ 的元素 $a + ub$ 的集合 J 在下列规则下是韦勃伦-魏德本体系：

1) $(a_1 + ub_1) + (a_2 + ub_2) = (a_1 + a_2) + u(b_1 + b_2)$.

2) 对于 $c \in F$，令 $(a + ub)c = ac + u(bc)$.

3) 对于 $z = a + ub$，$a, b \in F$，$b \neq 0$，和 $w = c + zd$，$c, d \in F$，令

$$wz = ds + z(c + dr) = ac + adr + ds + u(bc + bdr).$$

在这些规则下 J 是满足分配律 $(x + y)z = xz + yz$ 的韦勃伦-魏德本体系. 元素 $c \in F$ 具有性质 $cx = xc$，$c(xy) = (cx)y = (xc)y$. 其次，每个 $z \notin F$ 满足方程

$$z^2 - rz - s = 0.$$

证明. 加法有意义而且在加法下显然是阿贝尔群. 乘

---

1) 参看 M. Hall[2].

法有意义，但是存在着两种基本上不同的相乘规则 xy：关于 $y=c\in F$ 的规则 (2) 和关于 $y=z\notin F$ 的规则 (3). 分配律 $(x+y)z=xz+yz$ 成立，因为这些乘积当 $z\in F$ 时都可以用规则 (2) 计算，当 $z\notin F$ 时都可以用规则 (3) 计算，而这两个规则各自都满足分配律.

注意当 $z\notin F$ 时，规则 (3) 给出乘积 $z^2=rz+s$. 又当 $c\in F$ 时规则 (3) 给出 $cz=zc$. 显然当 $c, x\in F$ 时有 $cx=xc$，F 的单位元素 1 是 J 的单位元素. 为了证明在乘法下是络，必须证明在 $xy=v$ 内 x, y, v (都 $\neq 0$) 中的任何两个唯一决定第三个. 这时利用 $y\in F$ 时的规则 (2) 和 $y\notin F$ 时的规则(3)，就能得出 x 和 y 唯一决定 $xy=v$，又当 $x\neq 0$ 和 $y\neq 0$ 时，利用 (3) 中 $b\neq 0$ 和 $s\neq 0$ 的事实，易于验证 $v\neq 0$. 又给定 $y\neq 0$ 和 $v\neq 0$. 适当应用规则 (2) 或 (3) 就能唯一决定满足 $xy=v$ 的 $x\neq 0$.

在给定 $x\neq 0$ 和 $v\neq 0$ 时，情况稍稍有些复杂. 记 $x=a+ub$, $v=c+ud$, $a, b, c, d\in F$. 如果 $ad-bc=0$，则存在唯一的 $f\neq 0$, $f\in F$，使得 $af=c$ 和 $bf=d$，因而 $xf=v$，而且这是 F 中满足这个关系的唯一元素. 现在假定 $ad-bc\neq 0$，如果存在 $y=y_1+uy_2$, $y_1y_2\in F$, $y_2\neq 0$，则我们将有 $x=(a-by_1y_2^{-1})+y(by_2^{-1})$, $xy=sby_2^{-1}+y(a-by_1y_2^{-1}+rby_2^{-1})$ 和 $v=(c-dy_1y_2^{-1})+y(dy_2^{-1})$. 这时从 $xy=v$ 得出关系：

$$ay_2-by_1=d-rb,$$
$$cy_2-dy_1=sb.$$

因为 $ad-bc\neq 0$，这些方程有唯一的解 y_1 和 y_2，而且 $y_2=(d^2-rbd-sb^2)/(ad-bc)$，这里 $y_2\neq 0$，因为根据 x^2-rs-s 在 F 上不可约，当 F 的元素 d 和 b 都不是零时，我们不会有 $d^2-rbd-sb^2=0$，得到的 y_1 和 y_2 的值导出满足

$xy = v$ 的元素 $y \notin F$. 这证明了 J 的非零元素在乘法下组成络.

为了证明当 $m \neq n$ 时, $xn_1 = xn + v$ 有唯一的解, 只需要找出一个解, 因为假如存在两个解 x_1 和 x_2, 就将有 $(x_1 - x_2)m = (x_1 - x_2)n$ 而与在乘法下是络的性质矛盾. 当 m 和 n 都在 F 内时, 找一个解是容易的. 因此假定 $m \notin F$. (当 $m \in F, n \notin F$ 时,我们考虑 $xn = xm - v$.)我们可以用 m 来表出 n 和 V. 假定 $n = c \in F, v = v_1 + mv_2, v_1, v_2 \in F$. 如果 $x = x_1 + mx_2$, 则我们有

$$- cx_1 + sx_2 = v_1,$$

$$x_1 + (r - c)x_2 = v_2,$$

它是可解的,因为根据 $x^2 - rx - s$ 的不可约性,行列式 $c^2 - rc - s$ 不是零. 最后如果 $n = a + mb, v = v_1 + mv_2$ 而且我们令 $x = x_1 + mx_2$, 则就有 $- ax_1 + (a^2b^{-1} - ab^{-1}r - b^{-1}s + s)x_2 = v_1(1 - b)x_1 + ax_2 = v_2$.

这时行列式是 $- b^{-1}[a^2 - ra(1 - b) - s(1 - b)^2]$, 由于 $b \neq 0$ 而且 $x^2 - rx - s$ 是不可约的,它不会是零. 因此解存在而且 $xm = xn + v$ 有唯一的解 x. 总之 J 是韦勃伦-魏德本体系.

20.5. 茂芳平面和德沙格平面

在上一节里我们证明过,一个平面可以用韦勃伦-魏德本体系来建立坐标系, 必要而且只要它是相对于取作 L_∞ 的线的直移平面. 如果一个平面是相对于多过一条线的直移平面, 则关于它的坐标又能说些什么呢? 本节中就将回答这个问题.

定理 20.5.1. 如果平面 π 是相对于两条线的直移平面,

这两条线相交于点 Q，则它对于通过 Q 的线束中的每一条线都是平移平面.

推论 20.5.1. 如果 π 是相对于不共点的三条线的平移平面，则它是相对于每一条线的平移平面.

证明. 对于推论我们要指出的是,如果线族在包含了任意两条线时,就包含通过它们交点的线束,则这线族在包含了平面的三条不共点的线时,就必定包含平面的全部线.

假定 L_1 和 L_2 是相交于点 Y 的两条线，而且 π 是相对于 L_1 和 L_2 的平移平面. 设 L_3 是通过 Y 的第三条线而且 C 是 L_3 上与 Y 不同的任意点. 设 RCS 是通过 C 而且与 L_3 不同的线，它与 L_1 相交于 R 而且与 L_2 相交于 S. 于是存在具有轴 L_1 和中心 R 的合射 α，它把 S 变成 C 而且把 L_2 变成 L_3. 因为 π 具有以 L_2 为轴和以 S 为中心的所有合射,所以线性定理的图形对于以 S 为中心和以 L_2 为轴的所有情形都成立. 直射 α 把所有这些图形变成以 C 为中心和以 L_3 为轴的所有线性定理的图形. 因此在 π 上存在以 C 为中心和以 L_3 为轴的所有可能的合射. 因为这个论断对于 L_3 上不同于 Y 的每个点都成立,所以根据定理 20.4.4 的推论，π 是具有轴 L_3 的平移平面.

定理 20.5.2. 平面 π 对于通过点 $Y=(\infty)$ 的每条线都是平移平面,必要而且只要,(1)它的有限线由线性方程 $x=c$ 和 $y=xm+b$ 给出,(2)坐标满足下列定律.

2.1) 在加法下是阿贝尔群.

2.2) $(a+b)m=am+bm$.

2.3) $a(s+t)=as+at$.

2.4) 每个 $a\neq 0$ 都有逆 a^{-1}，使得 $aa^{-1}=1=a^{-1}a$.

2.5) $a^{-1}(ab)=b$.

证明. 假定 π 对于通过 $Y=(\infty)$ 的每条线都是平移

平面，这包括 L_∞，因而根据定理 20.4.6，我们得出线性条件(1) 满足，而且坐标组成韦勃伦-魏德本体系．这就给出定理中的条件 (2.1) 和 (2.2)．其余三个条件必须证明．

考虑具有中心 $Y=(\infty)$ 和轴 $x=0$ 的合射，它把点 (0) 映成点 (m)．

这时全体点 $(0, b)$ 是不变的，而且线 L_∞ 和 $x=c$ 是不变的，我们依次得出

$$(0)\rightarrow(m),$$
$$(0, b)\rightarrow(0, b),$$
$$y=b\rightarrow y=xm+b,$$
$$x=a\rightarrow x=a,$$
$$(a, b)\rightarrow(a, am+b).$$

这给出任意有限点的映射．

特别地 $$(1, t)\rightarrow(1, m+t)$$
而且 $$(0, 0)\rightarrow(0, 0),$$
因而 $$y=xt\rightarrow y=x(m+t),$$
但是 $$(a, at)\rightarrow(a, am+at),$$
而且因为 (a, at) 在 $y=xt$ 上，所以 $(a, am+at)$ 在 $y=x(m+t)$ 上，因而

$$am+at=a(m+t),$$

这就是分配律 (2.3)．

现在考虑具有中心 $(0, 0)$ 和轴 $x=0$ 的合射，它把 (0) 变成 $(-1-a, 0)$，这时

$$(0)\rightarrow(-1-a, 0),$$
$$(0, 1+a)\rightarrow(0, 1+a),$$
因而 $$y=1+a\rightarrow y=x+1+a.$$
$$(0)\rightarrow(-1-a, 0),$$
$$(0, b+ab)\rightarrow(0, b+ab),$$

因而 $$y = b + ab \to y = xb + b + ab.$$
$$y = 1 + a \to y = x + 1 + a,$$
$$y = x(1 + a) \to y = x(1 + a),$$
因而 $(1, 1 + a) \to (d, d + 1 + a)$ 假如 $a \neq 0$，这里 $d(1 + a) = d + 1 + a$.

又 $$(\infty) \to (\infty),$$
$$(1, 1 + a) \to (d, d + 1 + a),$$
因而 $$x = 1 \to x = d.$$
现在
$$y = x(b + ab) \to y = x(b + ab),$$
$$y = b + ab \to y = xb + b + ab,$$
因而 $$(1, b + ab) \to (d, d[b + ab]).$$
这里又有 $d(b + ab) = db + b + ab$.

这时我们假定，不仅 $a \neq 0$，而且 $(-1-a, 0) \neq (0, 0)$，即 $a \neq -1$. 对于这样的 a，存在 d，使得 $d(1 + a) = d + 1 + a$，而且对于任何 b，$d(b + ab) = db + b + ab$. 如果我们令 $d = u + 1$ 而且利用分配律，

则 $$ua = 1,$$
而且 $$u(ab) = b.$$
根据分配律我们直接得出，即使对于 $a = -1$，这些关系也成立，这时 $u = -1$. 因为当 $u \neq 0$ 时存在 v 使得
$$vu = 1$$
而且 $$v(ua) = a,$$
所以 $v = a$. 因此只要记 $u = a^{-1}$，就有定律 (2.4) $aa^{-1} = a^{-1}a = 1$ 和 (2.5) $a^{-1}(ab) = b$.

反之，假定条件(1)和(2)对于平面 π 的坐标成立，根据定理 20.4.6，我们知道 π 是相对于 L_∞ 的平移平面. 利用定理 20.5.1，只要证明 π 具有把 L_∞ 映成某条别的通过 $Y = (\infty)$

的线的直射.

下列映射就是这样的直射:

$$(\infty)\to(\infty),$$
$$(m)\to(1,m),$$
$$(-1,m)\to(-m),$$
$$(0,b)\to(0,b),$$
$$(c,d)\to[(1+c^{-1})^{-1},(1+c)^{-1}d],\quad c\neq 0,-1.$$
$$L_\infty\to x=1,$$
$$x=-1\to L_\infty,$$
$$x=0\to x=0,$$
$$x=c\to x=(1+c^{-1})^{-1},\ c\neq 0,-1.$$
$$y=xm+b\to y=x(m-b)+b.$$

为了证明这一点,必须证明关联性在映射下保持着;特别地,如果 (c,d) 在 $y=xm+b$ 上,则像点在像线上. 这可以简化成证明

$$(1+c)^{-1}(cm+b)=(1+c^{-1})^{-1}(m-b)+b$$

是恒等式. 这从定理中的定律得出,因为下列两个都是恒等式:

$$(1+c)^{-1}(cm)=(1+c^{-1})^{-1}m,$$
$$(1+c)^{-1}b=(1+c^{-1})^{-1}(-b)+b,$$

根据上述定律还可以证明由勃鲁克提出的又一个恒等式. 记:

$$[y^{-1}-(y+z^{-1})^{-1}][y(zy)+y]=t,$$

这里我们只排除值 $y=0$ 和 $y=-z^{-1}$. 那么用 $y+z^{-1}$ 去乘,我们得出

$$(y+z^{-1})t=(y+z^{-1})[zy+1$$
$$-(y+z^{-1})^{-1}(y(zy))-(y+z^{-1})^{-1}y]$$
$$=y(zy)+y+y+z^{-1}$$

$$-y(zy)-y=y+z^{-1}.$$

因此 $t=1$. 而且 $y^{-1}-(y+z^{-1})^{-1}$ 和 $y(zy)+y$ 是互逆的. 于是对于任何 x,

$$[y^{-1}-(y+z^{-1})^{-1}][(y(zy))x+yx]=x.$$

然后记

$$[y^{-1}-(y+z^{-1})^{-1}][y(z(yx))+yx]=w.$$

我们发现

$$(y+z^{-1})w=(y+z^{-1})[z(yx)+x)]$$
$$-y[z(yx)]-yx=yx+z^{-1}x$$
$$=(y+z^{-1})x.$$

因此 $w=x$. 现在来比较 w 和 x 的表达式,我们必须有

$$(M)\qquad [y(zy)]x=y[z(yx)],$$

这是茂芳恒等式. 这个恒等式对于被排除的值 $y=0$ 和 $y=-z^{-1}$ 显然成立,所以它是无例外地成立的. 特别地, $z=1$ 时茂芳恒等式简化成左交替律.

$(LA)\qquad (yy)x=y(yx).$

如果平面对于每条线都是平移平面,则它叫做**茂芳平面**,这是因为茂芳 (Moufang[1]) 最先研究它们.

定理 20.5.3. 平面是茂芳平面,必要而且只要每个三元环都是(1)线性的和(2)交替可除环,即满足下列定律:

2.1) 在加法下是阿贝尔群,

2.2) $(a+b)m=am+bm.$

2.3) $a(s+t)=as+at.$

2.4) 每个 a 都有逆 a^{-1} 满足 $a^{-1}a=aa^{-1}=1.$

2.5) $a^{-1}(ab)=b.$

2.6) $(ba)a^{-1}=b.$

外加交替律成立:

2.7) $a(ab)=(aa)b,\ (ba)a=b(aa).$

证明. 根据定理 20.5.3，我们有 (1) 以及 (2.1) 到 (2.5). 我们必须证明 (2.6)，因为显然右交替律 $(ba)a = b(aa)$ 从 (2.6) 得出，正像左交替律从 (2.5) 得出一样.

考虑具有轴 $y = 0$ 和中心 $(0, 0)$ 的合射，它把 $Y = (\infty)$ 映成 $(0, -1)$. 我们依次有:

$$(\infty) \to (0, -1),$$
$$(1, 0) \to (1, 0),$$

因而 $$x = 1 \to y = x - 1.$$
$$(\infty) \to (0, -1),$$
$$(a, 0) \to (a, 0),$$

因而 $$x = a \to y = xa^{-1} - 1.$$
$$x = 1 \to y = x - 1,$$
$$y = x(1 - ab) \to y = x(1 - ab).$$

于是 $$(1, 1 - ab) \to [(ab)^{-1}, (ab)^{-1} - 1].$$

又 $$(0) \to (0),$$

因而 $$y = 1 - ab \to y = (ab)^{-1} - 1.$$
$$x = a \to y = xa^{-1} - 1,$$
$$y = x(a^{-1} - b) \to y = x(a^{-1} - b),$$

因而 $$(a, 1 - ab) \to (b^{-1}, b^{-1}a^{-1} - 1).$$

因为 $$(0) \to (0),$$

所以我们有 $$y = 1 - ab \to y = b^{-1}a^{-1} - 1.$$

比较 $y = 1 - ab$ 的像，我们必须有
$$(ab)^{-1} = b^{-1}a^{-1}.$$
利用这个等式，我们发现，因为 $b^{-1} = a(a^{-1}b^{-1})$，
$$b = (b^{-1})^{-1} = [a(a^{-1}b^{-1})]^{-1}$$
$$= (a^{-1}b^{-1})^{-1}a^{-1} = (ba)a^{-1}.$$
这就证明了 (2.6).

我们现在证明了，在茂芳平面上，坐标满足以上关于交替

可除环的定律．反之，假定给了一个交替可除环．构造具有这些坐标的平面，根据定理 20.5.2，这平面对于通过 $Y=(\infty)$ 的每条线都是平移平面．因此根据定理 20.5.1 和它的推论，只要找出变动 $Y=(\infty)$ 的直射，就能得出这平面对于每条线都是平移平面，下列反射就是这样的直射：

$$(a, b) \rightleftarrows (b, a),$$
$$(0) \rightleftarrows (\infty),$$
$$(m) \rightleftarrows (m^{-1}),\ m \neq 0,$$
$$x = c \rightleftarrows y = c,$$
$$y = xm + b \rightleftarrows y = xm^{-1} - bm^{-1},\ m \neq 0.$$

这完成了定理的证明．下面提出一点注解．

比这里已证的更多的结论成立，但是证明要求比这里已给的为多的交替环的理论．这样的结论成立：如果平面对于两条不同的线是平移平面，则它是茂芳平面，即它对于每条线都是平移平面．在代数上这意思是说：定律(2.6)：$(ba)a^{-1}=b$ 是前几个定律的结果，这个事实的简单的证明是作者所没有见到的．我们看到，左交替律 $x(xy)=(xx)y$ 是 (2.5) 的结果．克林佛德 (Kleinfeld[2]) 和斯可尔涅可夫 (Skornyakov [Скорняков][2])曾证明，在特征不是 2 时，从这个定律(在可除环内) 还得出右交替律 $(yx)x=y(xx)$．这在特征为 2 时不成立．但是散·叟谢(San Soucie[1])证明了，利用较强的茂芳定律 $[y(zy)]x=y[z(yx)]$ (我们曾证明它是 (2.5) 的结果)，即使在特征为 2 时也能得出右交替律．勃鲁克和克林佛德 (Bruck and Kleinfold[1]) 研究了交替可除环 R 而且发现了意外的结果：这种环 R 或是可结合的，或是在它的中心(这是一个域 F) 上的特殊类型的代数．R 是 F 上的凯雷-狄克逊代数，这是具有八个基元素的代数，不在 F 内的任何一个元素生成 F 上的二次域，(不在 F 的同一个二次扩张内的) 任何两

个元素生成四元素代数．这个细节知识帮助他们证明：在茂芳平面上，以每个三元环作为坐标不仅产生一个交替可除环，而且产生的是同一个交替可除环． 读者可以从匹克尔的书(Pickert[1])中，看到除散·叟谢的工作以外的全部结果的完全的叙述．

定理 20.5.4. 在平面 π 上下列条件是等价的：

1) π 是 X-OY 传递的，即 π 具有以 $X=(0)$ 为中心和以 $x=0$ 为轴的所有透射．

2) 在 π 的由 X, Y, O, I 给定的三元环内，我们有

2.1) $x \cdot m \circ b = xm + b$，和

2.2) 在乘法下是群．

证明. 假定在 π 上(1)成立，考虑具有轴 $x=0$ 和中心 $X=(0)$ 的透射，它在 L_∞ 上使 $(m)\to(1)$．我们有

$$(0,0)\to(0,0),$$

$$(m)\to(1),$$

因而 $$y=xm\to y=x.$$

然而 $$y=am\to y=am,$$

因而 $$(a,am)\to(am,am).$$

因为 $$(\infty)\to(\infty),$$

所以 $$x=a\to x=am,$$

又 $$y=c\to y=c,$$

因而 $$(a,c)\to(am,c).$$

再有 $$(0,b)\to(0,b),$$

$$(m)\to(1),$$

因而 $$y=x\cdot m\circ b\to y=x+b.$$

因此如果 (a,c) 在 $y=x\cdot m\circ b$ 上，则 (am,c) 在 $y=x+b$ 上．因而从 $c=a\cdot m\circ b$ 得出 $c=am+b$，于是 $a\cdot m\circ b=am+b$，这就是线性条件(2.1)．

这时由 $(m)\to(1)$ 决定的透射使 $(a,1)\to(am,1)$，特别地有 $(1,1)\to(m,1)$. 如果我们继续施行使 $(n)\to(1)$ 的透射，则就有 $(1,1)\to(m,1)\to(mn,1)$ 和 $(a,1)\to(am,1)\to((am)n,1)$.

但是乘积必定是使 $(mn)\to(1)$ 的透射，因而 $(a,1)\to[a(mn),1]$，所以 $(am)n=a(mn)$，这就是乘法结合律. 而因为在乘法下是络，由此得出在乘法下是群.

现在假定 (2) 成立，那么对于固定的 $m\neq 0$，我们得出 π 上的下列透射：

$$
\begin{gathered}
(\infty)\to(\infty),\\
(0)\to(0),\\
(n)\to(m^{-1}n),\\
(a,b)\to(am,b),\\
L_\infty\to L_\infty,\\
x=a\to x=am,\\
y=xn+b\to y=x(m^{-1}n)+b.
\end{gathered}
$$

令 m 遍历 $\neq 0$ 的所有的值，我们得出具有中心 $X=(0)$ 和轴 $x=0$ 的所有透射. 因此从 (2) 得 (1).

定理 20.5.5. 在平面 π 上，如果德沙格定理的下列特殊情形成立：

1）在具有不共点的三条不同的轴的所有情形下的线性定理；

2）对于一条轴和不在轴上的一个中心的一般定理，

则 π 可以用结合可除环建立坐标. 这时德沙格定理在整个平面 π 上都成立. π 的直射群是在四点形上传递的，而且 π 的每个三元环都是同一个结合可除环.

证明. 根据假设，我们可以应用定理 20.5.3 和 20.5.4，而且对于在 π 上给定三元环的四点形 X,Y,O,I 的一个选

择，我们有 $x \cdot m \circ b = xm + b$，又全体坐标组成结合可除环．明显地，如果存在 π 的直射把四点形 X_1，Y_1，O_1，I_1 的点依次变成第二个四点形 X_2，Y_2，O_2，I_2 的点，则三元环是同构的．我们先来证明，如果平面 π 由关于四点形 X_1，Y_1，O_1，I_1 的结合可除环 D 建立坐标，则 π 的直射是在四点形上传递的，因而每个四点形所产生的坐标环都同构于 D．根据定理 20.5.3，π 相对于 π 上的每条线都是平移平面．给定三角形 ABC 而且取 AB 为轴，就存在合射不变 A 和 B 而把 C 变成不在 AB 上的任意 C'．以这个方式从任意四点形 X_2，Y_2，O_2，I_2 开始．适当应用这种合射，我们找到直射映 X_2 成 X_1，Y_2 成 Y_1 和 O_2 成 O_1．新的点 I_2 不能在三角形 $X_2Y_2O_2$ 的任何一条边上，因而在由 X_1，Y_1，O_1，I_1 决定的坐标里，这是个有限点 $I_2=(a,\ b)$，这里 $a \neq 0$，$b \neq 0$．下列直射不变 X，Y，O 而把 I_2 映成 I_1：

$$(x,\ y) \to (xa^{-1},\ yb^{-1}),$$
$$(m) \to (amb^{-1}),$$
$$(\infty) \to (\infty),$$
$$y = xm + s \to y = x(amb^{-1}) + sb^{-1},$$
$$x = c \to x = ca^{-1},$$
$$L_\infty \to L_\infty.$$

因而所有三元环产生同一个结合可除环 D，所以 π 是在四点形上传递的．

只留下证明德沙格定理在整个 π 上成立．如果中心在轴上，这当然成立，因为 π 具有所有可能的合射．现在假定中心不在轴上，取中心作为 O 而且取轴作为 L_∞．我们来证明 π 具有以 O 为中心和以 L_∞ 为轴的所有透射．对于固定的 $a \neq 0$，下面就是这样的透射：

$$(\infty) \to (\infty),$$

$$(m) \to (m),$$
$$(c, d) \to (ac, ad),$$
$$L_\infty \to L_\infty,$$
$$x = c \to x = ac,$$
$$y = xm + b \to y = xm + ab.$$
令 a 遍历不是 0 的所有值，就得出具有中心 O 和轴 L_∞ 的所有透射.

20.6. 魏德本定理和阿廷-左恩定理

我们在这里提出我们所需要的有限域的若干性质. 这些性质的证明可以参考范·德·瓦尔登的《近世代数学》[1]（van der Waerden[1],第一卷第五章 § 37).

1）有限域的元素数是素数的方幂. 对于任何素数方幂 p^r,存在具有 p^r 个元素的有限域 $GF(p^r)$，而且在同构下它是唯一的.

2）$GF(p^r)$ 的每个元素 x 都满足关系 $x^{p^r} = x$. $GF(p^r)$ 的除零外的 $p^r - 1$ 个元素的乘法群是循环群. 这个循环群的生成元素叫做本原根.

3）$GF(p^r)$ 可以表成系数在 p 个元素的域 F_p 内的多项式 $P(x)$ 以 F_p 上的一个 r 次不可约多项式 $f(x)$ 为模的剩余类. $GF(p^r)$ 也可以表成整系数多项式以理想 $[p, f(x)]$ 为模的剩余类.

4）$GF(p^r)$ 的全体自同构组成由自同构 $z \to x(z) = z^p$ 生成的 r 阶循环群.

定理 20.6.1（魏德本定理）. 有限除环 R 必定是可交换

1）新版改名《代数学》,科学出版社，(I) 1963，(II) 1976.——译者

的，因而是有限域 $GF(p^r)$.

证明. 下面的证明是由维特(Witt[1])提出的. R 的 1 生成 R 的特征子域，它必定是对于某个素数 p 的有限域 F_p. 设 R 在 F_p 上有由 r 个元素 $x_1=1, x_2, \cdots, x_r$ 组成的基底. 那么 R 恰好有 p^r 个元素. R 的中心 Z 由 R 的全体这样的元素 z 组成，它们对于每个 $x\in R$ 都有 $zx=xz$. Z 是 R 的交换子环，因而是有限域. 设 Z 有 $q=p^s$ 个元素. 我们希望证明 Z 是整个 R. R 在任何情况下都是 Z 上的向量空间，而且如果 R 在 Z 上具有由 t 个元素组成的基底，则 R 一共有 $q^t=p^{st}=p^r$ 个元素. 当 $R=Z$ 时就有 $t=1$. R 的元素 x 的正规化子 N_x 是包含 Z 的子环. 因此 N_x 包含 q^d 个元素，而且因为 R 是 N_x 上的向量空间，我们必须有 $d|t$. 因此，在 R 的除 0 外的 $p^r-1=q^t-1$ 个元素的乘法群 R^* 内，不在 Z 内的元素 x 具有阶为 q^d-1 的正规化子，这里 d 是 t 的约数而且 $d<t$. 计算 R^* 的元素，我们有

$$q^t-1=q-1+\Sigma(q^t-1)/(q^d-1), \quad (20.6.0)$$

这里 $q-1$ 是中心的元素数，而其余的每一加项计算的是一个共轭类的元素数 $(q^t-1)/(q^d-1)$，这里 $d|t$, $d<t$.

在 § 16.8 里证明过多项式 $f(x)=x^t-1$ 具有有理整系数因式 $k(x)=\Pi(x-w^j)$，这里 w 是 t 次本原单位根，而且 w^j, $1\leqslant j\leqslant t$, $(j,t)=1$, 是所有 t 次本原单位根. 那么如果 $d|t$, $d<t$, 则我们有 $x^t-1=k(x)(x^d-1)r(x)$，因为 $k(x)$ 不包含 x^d-1 的任何因式. 这里 $r(x)$ 包含 x^t-1 的所有其余的因式，假如这种因式存在的话. 因此 $(x^t-1)/(x^d-1)=k(x)r(x)$. 对于 $x=q$,

$$k(q)=\prod_{(i,j)=1}(q-w^j),$$

而且因为 $w^j\neq 1$ 是复数单位根，所以 $|q-w^j|>q-1$. 因

此 $k(q)$ 是绝对值大于 $q-1$ 的有理整数. 因此当 $t>1$ 时, $k(q)$整除(20.6.0)中除 $q-1$ 外的各项. 于是 $k(q)$也整除 $q-1$, 由于 $|k(q)|>q-1$, 这是不可能的. 因此唯一的可能是 $t=1$, 这就是说 $Z=R$,所以 R 是可交换的, 因而是有限域.

定理 20.6.2 (阿廷-左恩)[1]. 有限交替可除环是有限域 $GF(p^r)$.

证明. 我们先稍为展开一点交替环的理论. 交替环 R 是具有二元加法和乘法的体系, 其中 (1) 在加法下是阿贝尔群, (2) 两种分配律成立, (3) 乘法满足弱结合律

$$(xx)y=x(xy),\quad y(xx)=(yx)x. \tag{20.6.1}$$

如果 R 的非零元素在乘法下组成络, 则 R 是可除环. 我们在上一节里指出过, 茂芳平面可以用交替可除环建立坐标. 这时代替 (20.6.1), 我们有下列乘法定律:

$$aa^{-1}=a^{-1}a=1, \tag{20.6.2}$$
$$a^{-1}(ab)=b=(ba)a^{-1}.$$

我们证明过从定律 (20.6.2) 可以得出定律 (20.6.1).

在分配律成立的任何环里可以定义结合者 (x,y,z) 和换位子 (x,y). 它们用下列规则定义:

$$(x,y,z)=(xy)z-x(yz), \tag{20.6.3}$$
$$(x,y)=xy-yx.$$

因而结合者在任何结合环内恒等于零, 而换位子在任何交换环内恒等于零, 结合者和换位子对它的每个元都是线性的. 定律 (20.6.1) 可以改写成

$$(x,x,y)=0,\ (y,x,x)=0. \tag{20.6.4}$$

根据结合者的线性性质,我们有

$$0=(x,y+z,y+z)=(x,y,y)$$

---

1) 参看 Zorn[1].

$$+(x,y,z)+(x,z,y)+(x,z,z)$$
$$=(x,y,z)+(x,z,y), \qquad (20.6.5)$$
和
$$0=(x+y,x+y,z)=(x,x,z)$$
$$+(x,y,z)+(y,x,z)+(y,y,z)$$
$$=(x,y,z)+(y,x,z).$$
因此我们有
$$(x,y,z)=-(x,z,y)=(z,x,y)$$
$$=-(z,z,x)=(y,z,x)$$
$$=-(y,x,z). \qquad (20.6.6)$$
这是说(x, y, z)在x, y, z的对称群的置换的作用下是不被交替群所改变而被奇置换改变符号. 就是这个性质使我们把这种环叫做**交替环**. 从规则(20.6.6)立即得出$(x, y, x)=-(x, x, y)=0$, 因而
$$(xy)x=x(yx). \qquad (20.6.7)$$
定律(20.6.7)叫做**自反律**.

如果环内的函数$h(x_1, \cdots, x_n)$是(1)对于它的每个元都是线性的,(2)当它的任何两个元相等时为零,则它叫做**反对称的**. 我们看到从反对称性可以得出交替性质, 而且在交替环内,结合者和换位子都是对称的.

我们来推导在交替环内成立的几个公式. 将要给出比证明我们的定理所需要的更多的公式, 但是它们都是很值得在这里提出的. 下列恒等式可以证明是在具有分配律的任何环内都成立的:
$$(wx,y,z)-(w,xy,z)+(w,x,yz)$$
$$=w(x,y,z)+(w,x,y)z. \qquad (20.6.8)$$
我们用下列规则定义函数$f(w, x, y, z)$:
$$f(w,x,y,z)=(wx,y,z)-x(w,y,z)$$
$$-(x,y,z)w. \qquad (20.6.9)$$

引理 20.6.1. 在任何交替环 R 内，(20.6.9) 中的函数 $f(w, x, y, z)$ 是反对称的而且满足等式：

$$3f(w, x, y, z) = (w, (x, y, z)) - (x, (y, z, w)) + (y, (z, w, x)) - (z, (w, x, y)). \quad (20.6.10)$$

$$f(w, x, y, z) = ((w, x), y, z) + ((y, z), w, x). \quad (20.6.11)$$

证明. 根据 (20.6.6)，我们可以把 (20.6.8) 改写成

$$(wx, y, z) - (xy, z, w) + (yz, w, x) = w(x, y, z) + (w, x, y)z. \quad (20.6.12)$$

从 (wx, y, z) 减去由 (20.6.9) 给出的 f 的表达式中的各项，而且对于 (20.6.12) 左边其他的项也这样处理，我们得出

$$f(w, x, y, z) - f(x, y, z, w) + f(y, z, w, x) = F(x, y, z, w), \quad (20.6.13)$$

这里 $F(x, y, z, w)$ 是 (20.6.10) 的右边，因而当它的元循环置换时要改变符号. 因此根据 (20.6.13)，

$$0 = F(w, x, y, z) + F(x, y, z, w) = f(w, x, y, z) + f(z, w, x, y),$$

于是

$$f(w, x, y, z) = -f(z, w, x, y). \quad (20.6.14)$$

因此 f 在它的元循环置换时改变符号，而根据 (20.6.9)，f 在它的后两个元交换时改变符号，因此 f 在它的任何两个元交换时改变符号. 因为 $f(w, x, y, z)$ 在有两个元相等时等于 0，所以 f 是反对称的. 特别地，(20.6.13) 简化成 (20.6.10). 从 (20.6.8) 减去交换 w 和 x 的结果得出

$$((w, x), y, z) = -(w, (x, y, z)) + (x, (y, z, w)) + 2f(w, x, y, z).$$

因而计算 (20.6.11) 的右边而且利用 (20.6.10) 就能得出

(20.6.11) 的左边.

引理 20.6.2. 对于交替环的所有 x, y, z 都有

$$(x^2, y, z) = x(x, y, z) = (x, y, z)x, \quad (20.6.15)$$

$$(x, xy, z) = x(x, y, xz) = (x, y, z)x, \quad (20.6.16)$$

$$(x, yx, z) = (x, y, zx) = x(x, y, z), \quad (20.6.17)$$

以及茂芳恒等式

$$(xy)(zx) = x((yz)x) = (x(yz))x. \quad (20.6.18)$$

$$x(y(xz)) = ((xy)x)z, ((zx)y)x = z(x(yx)). \quad (20.6.19)$$

证明. 我们从 $f(x, x, y, z) = 0$ 得出 (20.6.15). 考虑 $f(x, y, z, x) = 0$ 和 $f(x, z, x, y) = 0$ 可以得出 (20.6.16) 的两部分. 同理从 $f(y, x, x, z) = 0$ 和 $f(z, x, x, y) = 0$ 得出 (20.6.17). 为了证明 (20.6.18), 我们注意到, 根据 (20.6.17),

$$\begin{aligned}(xy)(zx) &= x(y(zx)) + (x, y, zx) \\ &= x(y(zx)) + x(y, z, x) \\ &= x((yz)x).\end{aligned}$$

(20.6.19) 的第一个等式可以根据 (20.6.16) 而导出

$$\begin{aligned}((xy)x)z &= (xy)(xz) + (xy, x, z) \\ &= x(y(xz)) + (x, y, xz) - (x, xy, z) \\ &= x(y(xz)).\end{aligned}$$

第二个等式可以同样地根据 (20.6.17) 导出.

现在可以来证明定律 (20.6.2) 在可除环内从定律 (20.6.1) 得出. 给定元素 $a \neq 0$, 则就存在 u 使 $au = 1$. 于是 $a = (au)a = a(ua)$, 因而也有 $ua = 1$, 于是只要记 $u = a^{-1}$, 就有 $a^{-1}a = aa^{-1} = 1$. 给定任何不是零的 a, b, 从关系 $b = a^{-1}c$ 决定 c. 那么利用 (20.6.19) 的第一个等式

$$\begin{aligned}a^{-1}(ab) &= a^{-1}(a(a^{-1}c)) = ((a^{-1}a)a^{-1})c \\ &= (1a^{-1})c = a^{-1}c = b.\end{aligned}$$

同理，从(20.6.19)的第二个等式得出 $(ba)a^{-1}=b$.

现在我们有了足够的关于交替环的知识来证明阿廷-左恩定理了. 设 R 是有限的交替环. 只要证明由两个元素 b 和 c 生成的有限可除环 R_1 是结合的. 因为然后根据魏德本定理，R_1 是有限域而且由单独一个元素 d 生成. 因此，如果 R 由 $b_1, b_2, \cdots, b_s$ 生成，则 b_1, b_2 生成有限域，而且它由单个元素 c_1 生成. 于是 R 由 $c_1, b_3, \cdots, b_s$ 生成. 继续下去，我们可以减少生成元素的个数直到 R 本身由单个元素生成，因而它是结合的，因而它是有限域 $GF(p^r)$.

考虑由 b 和 c 生成的 R_1，这里 R_1 是 R 的在加法和乘法下闭合的子体系. R_1 是有限的而且没有零因子. 设 $a_1, \cdots, a_t$ 是 R_1 中不是零的元素. 那么对于 $x\in R_1$, $xa_1, \cdots, xa_t$ 全不相同，因为 R_1 不包含零因子，因而这些元素是以某个顺序排列的 $a_1, \cdots, a_t$. 因此对于某个元素例如 a_1，我们有 $xa_1=x$，于是 $a_1=1$ 是 R 的单位元素. 又对于某个 a_i 有 $xa_i=1$，因而 $a_i=x^{-1}$. 因此 R_1 是可除环. R_1 的元素是若干单项式 $(x_1\cdots x_r)(x_{r-1}\cdots x_n)$ 的和，这里每个 x_i 是 b 或 c 而且各项是以任意方式加括弧的. 因为两个分配律都成立，乘法在 R_1 中可结合，必要而且只要单项式的乘法可结合. 为了证明这一点，我们用下列规则递归地定义正规(或左括弧)单项式:

$$[x_1x_2]=x_1x_2 \tag{20.6.20}$$

$$[x_1\cdots x_n]=[x_1\cdots x_{n-1}]x_n.$$

如果能证明任意加括弧的单项式等于正规单项式，则结合律就成立了，因为那时将有

$$\begin{aligned}&([x_1\cdots x_r][y_1\cdots y_s])[z_1\cdots z_t]\\&=[x_1\cdots x_ry_1\cdots y_sz_1\cdots z_t]\\&=[x_1\cdots x_r]([y_1\cdots y_s][z_1\cdots z_t]).\end{aligned}$$

对于每个单项式等于具有依次相同的因子的正规单项式，我

们对单项式的长度施行归纳法来证明. 根据(20.6.4)和(20.6.6), 对于 b 和 c 的长度为三的单项式, 由于它们必定包含重复因子,所以这个结合律成立,即

$$x_1(x_2x_3) = (x_1x_2)x_3 = [x_1x_2x_3]. \qquad (20.6.21)$$

我们需要证明

$$[u_1\cdots u_r][v_1\cdots v_s] = [u_1\cdots u_rv_1\cdots v_s], \qquad (20.6.22)$$

我们对 $n = r + s$ 施行归纳法,而且对于固定的 n, 还对于 s 施行规纳法,当 $s = 1$ 时, 这就是定义(20.6.20). 假定 $s > 1$ 而且 $v_1 = v_s = b$ 或 $v_1 = v_s = c$. 那么在(20.6.19)的第二个恒等式 $z[x(yz)] = [(zx)y]x$ 内取 $z = [u_1\cdots u_r]$, $v_1 = v_s = x$ 和 $[v_2\cdots v_{s-1}] = y$, 就得出

$$[u_1\cdots u_r][xv_2\cdots v_{s-1}x] = \{([u_1\cdots u_r]x)[v_2\cdots v_{s-1}]\}x$$
$$= [u_1\cdots u_rv_1v_2\cdots v_{s-1}]v_s = [u_1\cdots u_rv_1v_2\cdots v_{s-1}v_s], \qquad (20.6.23)$$

这时用到了归纳假设, 而且最后证明了 $v_1 = v_s$ 时的(20.6.22). 现在假定 $v_1 \neq v_s$, 不妨假定 $v_1 = b$, $v_s = c$. 这时 u_r 是 b 或 c. 如果 $u_r = b$, 记

$$x = [u_1\cdots u_{r-1}],\ u_r = b,\ v_1 = b,\ [v_2\cdots v_s] = y.$$

那么

$$f(x, b, b, y) = 0 = (xb, b, y)$$
$$- b(x, b, y) - (x, b, b,)y.$$

这里 $(x, b, b) = 0$, 而且根据关于长度的归纳假设, x, b 和 y 是可结合的, 因而 $(x, b, y) = 0$. 因此 $(xb, b, y) = 0$, 于是 $(xb)(by) = [(xb)b]y$ 或

$$[u_1\cdots u_{r-1}b][bv_2\cdots v_3] = ([u_1\cdots u_{r-1}b]b)[v_2\cdots v_s]$$
$$= [u_1\cdots u_{r-1}bb][v_2\cdots v_s] = [u_1\cdots u_rv_1\cdots v_s], \qquad (20.6.24)$$

在最后一步用到了关于 s 的归纳假设.

同理,如果 $u_r = c$, 则记

$$x=[u_1\cdots u_{r-1}],\ u_r=c,\ [v_1\cdots v_{s-1}]=z\quad v_s=c.$$

现在 $f(x,c,z,c)=0=(xc,z,c)-c(x,z,c)-(c,z,c)x$. 这里 $(c,z,c)=0$ 而且根据关于长度的归纳假设, $(x,z,c)=0$, 因而 $(xc,z,c)=0$, 这给出 $(xc)(zc)=[(xc)z]c$ 或

$$\begin{aligned}[u_1\cdots u_{r-1}c][v_1\cdots v_{s-1}c]&=([u_1\cdots u_{r-1}c][v_1\cdots v_{s-1}])c\\&=[u_1\cdots u_{r-1}u_rv_1\cdots v_{s-1}]c\\&=[u_1\cdots u_{r-1}cu_rv_1\cdots v_{s-1}v_s].\end{aligned}\qquad(20.6.25)$$

等式(20.6.23)至(20.6.25)在所有情形确立了(20.6.22). 因此 R_1 的结合性证明了,这就证明了我们的定理.

20.7. 二重传递群和准域

有一类群与射影平面密切有关. 这就是一类二重传递群,它只有单位元素不变两个文字. 我们需要一个外加的假设,它虽然可能不是必要的,但却是我们的证明所要求的. 这就是下列定理中的条件(3)或(3′).

定理 20.7.1. 假定 G 是在文字 $c_0, c_1, \cdots, c_{n-1}$ 上的置换群, 满足

1) G 是二重传递的.

2) 只有单位元素不变两个文字.

3) 最多有一个把 c_i 变成 c_j 的元素变动全体文字, 或

(3′) n 是有限的.

那么单位元素和 G 中变动全体文字的元素组成传递的正规阿贝尔子群 A. G 同构于准域 K 中的线性代换 $x\to xm+b$ 的群. 反之,准域 K 中的线性代换 $x\to xm+b(m\neq 0)$ 产生满足(1)和(2)的群, 这时把线性代换看作 K 的元素上的置换. 如果对于 $m\neq 0, 1$, $xm+b=x$ 总有解, 则(3)满足,

因而我们可以取 $x = c$ 和 $y = xm + b$ 作为由准域 K 建立坐标的平面的有限的线. G 中的置换

$$\begin{pmatrix} c_0, c_1, \cdots, c_{n-1} \\ d_0, d_1, \cdots, d_{n-1} \end{pmatrix}$$

看作 K 的元素的置换,对应于 π 的线,它的点是 (c_i, d_i), $i = 0, \cdots, n-1$.

证明. 我们先证明定理中的纯群论的部分,我们希望证明单位元素和 G 中变动全体文字的元素组成传递的正规阿贝尔子群. 我们来证明几个引理.

引理 20.7.1. 在 G 中存在唯一的二阶元素, 它交换特定的一对文字 (i, j).

因为 G 是二重传递的, 这样的元素 g 必定存在. 这时 g^2 不变两个文字, 因而是 1. 具有这个性质的第二个元素 h 将使 gh^{-1} 不变两个文字,因而 $gh^{-1} = 1$, $g = h$.

引理 20.7.2. 2 阶元素属于同一个共轭类.

2 阶元素最多不变一个文字,当 $n = 2$ 时,只存在一个元素. 如果 $n \geqslant 3$, 则 2 阶的 g 和 h 必定同时改变某个元素 i, $g = (i, j)\cdots$, $h = (i, k)\cdots$. G 中的 $x = \begin{pmatrix} i, j, \cdots \\ i, k, \cdots \end{pmatrix}$ 将使 $x^{-1}gx = (i, k)\cdots = h$. 如果 2 阶元素的类里有任何元素不变一个文字, 则所有 2 阶元素都是如此. 我们可以分成两种情形:

情形 1. 2 阶元素改变所有的文字,

情形 2. 每个 2 阶元素都不变一个文字.

引理 20.7.3. 在情形 2 里, 存在唯一的 2 阶元素不变一个给定的文字.

像前面一样; $g = (i, j)\cdots$ 被 $x = \begin{pmatrix} i, j, \cdots \\ i, k, \cdots \end{pmatrix}$ 变成 $h=$

$(i, k)\cdots$. 但是如果 g 和 h 都不变同一个文字 s，则 x 必定也不变 s，因而 $x \neq 1$ 不变 i 和 s 而与假设 (2) 矛盾，又如果 g 不变文字 s，则用把 s 变成 t 的任意元素来作 g 的变形，就得出不变特定文字 t 的二阶元素.

注意从这个引理得出，如果 $g = (ij)(s)\cdots$，则 g 在不变 s 的子群 H_s 的中心内.

引理 20.7.4. 两个不同的 2 阶元素的乘积是变动所有文字的元素.

设 $g^2 = 1$，$h^2 = 1$，$g \neq h$. 假定相反地 gh 不变一个文字 i. 根据引理 20.7.3，g 和 h 不能同时不变 i，因而都不能不变 i. 于是我们将有 $g = (i, j)\cdots$，$h = (j, i)\cdots$，而且 $gh = (i)(j)\cdots = 1$，因而 $g = h$ 而与假设矛盾. 因此 gh 不能不变任何文字.

引理 20.7.5. 在 G 中存在唯一的变动全体文字的元素，它把给定的 i 变成给定的 $j \neq i$.

在情形 1 里元素 $g = (i, j)\cdots$ 就是这样的一个元素. 在情形 2 里，取 2 阶元素 $g = (i)\cdots$ 和 $h = (i, j)\cdots$，根据引理 20.7.4，gh 把 i 变成 j 而且变动所有的文字. 因此这种元素至少存在一个. 假设 (3) 是说最多存在一个这种元素. 我们发现从假设 (3) 得出引理 20.7.5. 因为 G 是 n 个文字上的二重传递群，所以不变一个文字 c_0 的子群有指数 n，而且不变 c_0 的子群 H_0 是在其余 $n-1$ 个文字上传递的. 于是因为只有单位元素不变两个文字，所以 H_0 的阶是 $n-1$. 因此 G 的阶是 $n(n-1)$. 因此把 i 变成 j 的元素组成不变 i 的子群 H_i 的左傍系，因而这种元素恰好有 $n-1$ 个. 对于给定的三个文字 i, j, k，根据二重传递性，在 G 内存在唯一的元素

$$g = \begin{pmatrix} i, k\cdots \\ j, k\cdots \end{pmatrix},$$

因为只有单位元素不变两个文字. 对于给定的 i, j, 恰好有 $n-2$ 种可能来选取 k, 因而在把 i 变成 j 的 $n-1$ 个元素中恰好存在一个元素变动所有的文字.

引理 20.7.6. 在情形 1 里变动所有文字的每个元素是 2 阶的, 而且它们与单位元素共同组成正规的阿贝尔子群.

显然 $g=(i, j)\cdots$ 是把 i 变成 j 而且变动全体文字的一个(因而是唯一)元素. 如果 $g^2=1$, $h^2=1$, 则当 $g=h$ 时, $gh=1$, 而当 $g \neq h$ 时, gh 是变动全体文字的 2 阶元素, $(gh)^2=1$, 因而 $hg=gh$, 所以 2 阶元素与单位元素共同组成阿贝尔群 A. 根据引理 20.7.2, A 是正规子群. 这证明了引理.

引理 20.7.7. 在情形 2 里, 变动全体文字的已知元素 g 可以表成两个 2 阶元素的乘积 $g=ab$, 这里 a 或 b 可以任意选取.

假证 $a^2=1$, a 不变文字 i 而且 g 把 i 变成 j, 取 $b=(i, j)\cdots$; 那么 $b^2=1$ 和 $g=ab$, 因为 ab 变动全体文字而且把 i 变成 j. 同理, 假定给了 g 和 b, $b^2=1$ 而且 b 不变 k. 如果 g 把 i 变成 k, 则只要取 $a=(i, k)\cdots$, 就有 $g=ab$.

引理 20.7.8. 在情形 2 里, 三个 2 阶元素的乘积 abc 也是 2 阶的而且 $abc=cba$.

如果 $a=b$, 引理是显然的. 如果 $b \neq a$, 则 $ab=g=dc$, 这里根据引理 20.7.7, $d^2=1$. 因此 $abc=dc^2=d$. 因为 $d=d^{-1}$, 所以 $abc=c^{-1}b^{-1}a^{-1}=cba$.

引理 20.7.9. 在情形 2 里, 变动全体文字的元素和单位元素共同组成正规的阿贝尔子群.

设 g 和 h 变动全体文字. 根据引理 20.7.4 和 20.7.7, $g=ab$, $h=cd$, 这里 a, b, c, d 都是 2 阶的. 记 $h=eb$, $e^2=1$, 我们有 $gh^{-1}=ae$, 因而当 $e=a$ 时, $gh^{-1}=1$, 而当 $a \neq e$

时，gh^{-1} 变动全体文字．因此变动全体文字的元素和单位元素共同组成子群 A．利用引理 20.7.8，

$$gh = (abc)d = (cba)d = c(bad) = c(dab) = hg,$$

因此群 A 是阿贝尔群．因为变动全体文字的元素的共轭元素也变动全体文字，所以 A 是正规子群．

我们现在来构造一个代数体系 S，它的元素是 G 所置换的文字 $c_0, c_1, \cdots, c_{n-1}$．我们任意地把其中一个记做 0，另一个记做 1，例如令 $c_0 = 0$，$c_1 = 1$．在 S 内定义加法

$$y = x + b, \tag{20.7.1}$$

必要而且只要在子群 A 内存在置换

$$A_b = \begin{pmatrix} 0, & \cdots, & x, & \cdots \\ b, & \cdots, & y, & \cdots \end{pmatrix}. \tag{20.7.2}$$

在 S 内定义乘法

$$y = xm, \tag{20.7.3}$$

必要而且只要在不变 0 的子群 H_0 内存在置换

$$M_m = \begin{pmatrix} 0, & 1, & \cdots, & x, & \cdots \\ 0, & m, & \cdots, & y, & \cdots \end{pmatrix}. \tag{20.7.4}$$

因为在 A 内存在唯一的把 0 变成 b 的元素，所以加法有意义．因为在 H_0 内存在唯一的把 1 变成 $m \neq 0$ 的元素，所以用 $m \neq 0$ 作乘法有意义．如果我们在 A 内有

$$A_a = \begin{pmatrix} 0, & \cdots, & x, & \cdots \\ a, & \cdots, & y, & \cdots \end{pmatrix}, \tag{20.7.5}$$

$$A_b = \begin{pmatrix} 0, & \cdots, & a, & \cdots, & y, & \cdots \\ b, & \cdots, & c, & \cdots, & z, & \cdots \end{pmatrix},$$

则

$$A_aA_b = A_c = \begin{pmatrix} 0, & \cdots, & x, & \cdots \\ c, & \cdots, & z, & \cdots \end{pmatrix}. \tag{20.7.6}$$

从加法的定义有

$$c=a+b,\ y=x+a,\ z=y+b,\ z=x+c. \quad (20.7.7)$$

这给出

$$(x+a)+b=x+(a+b), \quad (20.7.8)$$

这是加法结合律. 显然单位元素是

$$A_0=\begin{pmatrix}0, & 1, & \cdots, & x, & \cdots \\ 0, & 1, & \cdots, & x, & \cdots\end{pmatrix},$$

而且我们有定律

$$x+0=0+x=x. \quad (20.7.9)$$

其次,如果 u 使 $A_u=\begin{pmatrix}0, & \cdots, & a, & \cdots \\ u, & \cdots, & 0, & \cdots\end{pmatrix}$, 则 $a+u=0$ 因而 $u=-a$. 再有,因为 A 是阿贝尔群,所以如果 $A_aA_b=A_bA_a=A_c$, 则

$$c=a+b=b+a, \quad (20.7.10)$$

即加法是可交换的. 因此在加法下是阿贝尔群, 而且只要令 $a \rightleftarrows A_a$, 加法下的群 S 同构于 A.

以同样的方式利用 H_0 的置换,我们可以证明 S 的非零元素在乘法下组成群. 对于零总有规则 $0\cdot m=0$, 而且我们令 $m0=0$ 和 $00=0$, 现在设 g 是 G 的任意置换. 当 $(0)g=b$ 时,记 $g_1=gA_b^{-1}$. 那么 g_1 不变 0 因而是 H_0 的元素, 设 $g_1=M_m$. 于是

$$g=M_mA_b. \quad (20.7.11)$$

这时如果 $(x)g=y$, 则

$$(x)g=y=xm+b,\ m\neq 0. \quad (20.7.12)$$

表达式(20.7.11)是唯一的, 因为单位元素是 A 和 H_0 的唯一公共元素; 因而根据(20.7.12), G 的置换必定是 S 内的线性代换:

$$x\to xm+b,\ m\neq 0. \quad (20.7.13)$$

我们指出下列关系:

$$M_m M_t = M_{mt}, \quad (20.7.14)$$

$$M_m^{-1} A_1 M_m = A_m.$$

第一个是显然的，第二个是因为 $M_m^{-1}A_1M_m$ 变动全体文字而且把 0 变成 m，因而它必须是 A_m. 于是

$$M_t^{-1} A_m M_t = A_{mt}, \quad (20.7.15)$$

或者以对 S 的作用来表出是

$$(xt^{-1} + m)t = x + mt. \quad (20.7.16)$$

在这个式子里令 $x = yt$，我们得出

$$(y + m)t = yt + mt. \quad (20.7.17)$$

这是右分配律. 因此在 S 内，在加法下是阿贝尔群. 非零元素在乘法下是群，而且右分配律 (20.7.17) 成立. 因此 S 是准域，而 G 的置换是 S 内的线性代换:

$$x \to xm + b, \ m \neq 0, \quad (20.7.18)$$

这里根据准域的定律，如果 $\alpha: x \to xm_1 + b_1$ 和 $\beta: x \to xm_2 + b_2$，则

$$\alpha\beta: x \to (xm_1)m_2 + b_1m_2 + b_2. \quad (20.7.19)$$

反之，假定给了准域 S. S 的线性代换 (20.7.18) 在 (20.7.19) 的合成规则下组成群 G. 设 $r \neq s$ 是 S 的两个不同的元素. 那么

$$g: x \to x(r - s) + s \quad (20.7.20)$$

是 G 的元素使 $(0)g = s$ 和 $(1)g = r$. 因此 G 是二重传递的. G 的不变两个文字的元素共轭于不变 0 和 1 的元素. 但是如果 $x \to xm + b$ 不变 0 和 1，我们依次得出 $b = 0$，$m = 1$，因而这是单位元素. 因此唯有单位元素是 G 的不变两个文字的元素. 代换 $x \to x + (c - b)$ 变动全体文字而且把给定的 b 变成给定的 c. 如果 $xm + b = x$ 对于 $m \neq 0$ 和 1 总有解，则变动全体文字的置换只是加法 $x \to x + t$，而且其中只有 $x \to x + (c - b)$ 把给定的 b 变成给定的 c. 因此 (3)

成立．于是 $(xm+b)r=xr$ 或 $xs+t=xr$ 总有解（它显然是唯一的），这正好是这样的条件：看作韦勃伦-魏德本体系的 S 是平面的坐标系，这平面的有限线是 $x=c$ 和 $y=xm+b$，这就完成了定理各部分的证明．

我们注意到当 G 是有限的置换群时，条件（3）自动成立，因此决定只有单位元素不变两个文字的全体有限的二重传递群，相当于决定全体有限准域，蔡森豪斯（Zassenhaus[2]）做了这样的工作．我们现在来讨论这一点．

设 K 是有限准域．如果 K 内的乘法是可交换的，则 K 满足两个分配律，因而是有限域 $GF(p^r)$．这种可能性不再需要进一步的讨论．因而在这里我们可以假定 K 内的乘法是不可交换的．在这种情形里左分配律不可能成立，因为根据魏德本定理，那时 K 将是有限的结合可除环，因而是有限域 $GF(p^r)$．我们使用前面的定理的记号．K 是具有 n 个元素的有限准域，G 是 n 次的二重传递群，其中只有单位元素不变两个文字．G 是线性代换的群：

$$g: x \rightarrow xm+b,\ m \neq 0. \qquad (20.7.21)$$

A 是 G 的由单位元素和 G 中变动全体文字的元素组成的阿贝尔正规子群．$H_0=M$ 是不变文字 0 的子群．A 是 K 的加法群，M 是 K 的 $n-1$ 个非零元素的集合 K^* 的乘法群．

引理 20.7.K1. A 是初等阿贝尔群而且 n 是素数的方幂 $n=p^r$．A 的 $\neq 1$ 的元素在 M 下是共轭的．

A 是阿贝尔群，而且根据（20.7.14），$A_m=M_m^{-1}A_1M_m$．因而 A 的全体 $\neq 1$ 的元素在 M 下是共轭的．于是因为 A 必定包含素数 p 阶的某个元素，所以 A 的全体 $\neq 1$ 的元素都是 p 阶的，即 A 是初等阿贝尔群．因为 A 是正则的而且有阶 n，所以 $n=p^r$．

引理 20.7.K2. M 的元素是 A 的自同构，而且每个 $\neq 1$

的自同构仅不变K的元素 0.

M的元素是K的元素的置换 $a\to am$，而且其中每个 $\neq 1$ 的元素是加法群A的只不变元素 0 的自同构.

引理 20.7.K3. 如果 q 和 s 都是素数，则M的阶为 q^2 或 q^s 的子群必定是循环群.

我们先指出，当 $(x_1, \cdots, x_k)$ 是以置换表出的 M_m 中的一个圈，则 $x_1m=x_2$, $x_2m=x_3$, $\cdots$, $x_km=x_1$，因而 $(x_1+\cdots+x_k)m=x_1+\cdots+x_k$，所以当 $m\neq 1$ 时，我们有 $x_1+\cdots+x_k=0$. 现在假定M有 q^2 阶的子群W不是循环子群，因而是两个 q 阶群的直积. 设W由元素 x 和 y 生成，考虑W的一个传递组，它必定具有 q^2 个文字；元素 x 和 y 将有形状

$$x=(a_1a_2\cdots a_q)(a_{q+1}\cdots a_{2q})\cdots(a_{q^2-q+1}\cdots a_{q^2}),$$

$$y=(a_1, a_{q+1}, a_{2q+1}\cdots, a_{q^2-q+1})$$
$$\cdots(a_i, a_{q+i}, \cdots, a_{q^2-q+i}).$$

这时 xy^j 将有如下的包含 a_1 的传递组:

$$(a_1, a_{2+jq}, a_{3+2jq}, \cdots, a_{q+j(q-1)q}).$$

因此从观察各个圈得出

$$a_1+a_{2+jq}+\cdots+a_{q+j(q-1)q}=0. \qquad (20.7.22)$$

$$a_1+a_{q+1}+a_{2q+1}+\cdots+a_{q^2-q+1}=0. \qquad (20.7.23)$$

(20.7.22) 对 $j=0, 1, \cdots, q-1$ 求和再加上(20.7.23)，我们看到每个 $a_i\neq a_1$ 出现一次而 a_1 出现 $q+1$ 次. 因此

$$qa_1+(a_1+a_2+\cdots+a_{q^2})=0. \qquad (20.7.24)$$

但是对 x 的所有的圈求和，我们有

$$a_1+a_2+\cdots+a_{q^2}=0, \qquad (20.7.25)$$

因而

$$qa_1=0. \qquad (20.7.26)$$

由于M是 $n-1=p^r-1$ 阶的，所以 q 与 p 互素，因而(20.7.26)将产生矛盾的结果 $a_1=0$. 因此M不能包含 q^2 阶的非循环

子群.

同理,如果M包含q^s阶的非循环子群W,这里$q < s$,则W由这样的元素x和y生成:

$$x^s = 1,\ y^q = 1,\ q|s-1, \qquad (20.7.27)$$
$$y^{-1}xy = x^t,\ t^q \equiv 1(\mathrm{mod}\, s).$$

因为M是正则群,所以W有包含q^s个文字的传递组. W包含一个s阶子群和s个q阶子群. 考虑这些群中各一个包含已知文字a_1的圈:

$$(a_1 a_2 \cdots a_s)$$
$$(a_1 b_{11} \cdots b_{1,q-1})$$
$$(a_1 b_{21} \cdots b_{2,q-1})$$
$$\cdots\cdots\cdots$$
$$(a_1 b_{s1} \cdots b_{s,q-1})$$

q^s个文字除a_1以外, 在这些圈中只出现一次, 而a_1则出现$s+1$次. 但是因为全体q^s个文字是一个元素(例如x)的所有的圈中的文字,它们的和是零. 因此我们得出$sa_1 = 0$,于是因为$s|p^r-1$,我们将有$a_1 = 0$,这是个矛盾. 因此M不能包含q^s阶的非循环的子群.

引理 20.7.*K*4. M的奇数阶的西罗子群是循环群. M的西罗 2 子群或是循环群,或是广义的四元数群.

我们在定理 12.5.2 里证明过,对于奇数p,如果p群P不包含p^2阶的非循环子群,则P是循环群. 当$p=2$时,P或者是循环群,或者是广义的四元数群.

我们假定M有循环子群C使M/C也是循环群. 根据引理 20.7.K4 和定理 9.4.3, M必定有这个性质, 除非它具有西罗 2 子群是广义的四元数群, 而且当M是广义四元数子群和一个奇数阶群的直积时它也有这个性质. 定理 20.7.2 在M具有这个性质的情形给出全体有限准域K. 蔡森豪斯证明了,

确实存在七个其他的有限准域；我们将把它们列出．至于证明则可以参看蔡森豪斯原来的文章．

定理 20.7.2. 设 $q=p^h$ 是素数 p 的方幂，而且 v 是全部素因子都整除 $q-1$ 的整数，这里我们还要求当 $q\equiv 3(\text{mod}4)$ 时有 $v\not\equiv 0(\text{mod}4)$．那么对于 $hv=r$，我们可以用下列方式从有限域 $GF(p^r)$ 构造具有 $n=p^r$ 个元素的准域 K：

1）取 $GF(p^r)$ 的元素作为 K 的元素．

2）取 $GF(p^r)$ 内的加法作为 K 内的加法．

3）K 内的乘积 $w\circ u$ 以下列方式用 $GF(p^r)$ 内的乘积 $x\cdot y$ 来定义：

设 z 是 $GF(p^r)$ 的一个取定的本原根，则当 $u=z^{kv+j}$ 时，用 $q^i\equiv 1+j(q-1)[\text{mod}v(q-1)]$ 可以唯一决定取模 v 的整数 i．我们用下列规则定义乘积 $w\circ u$：

$$w\circ u=u\cdot w^{q^i}.$$

4）K 的中心是 $GF(q)$．

如果准域 K 具有 $n=p^r$ 个元素，而且它的乘法群 M 具有正规循环子群 C 使 M/C 是循环群，则 K 可以用上述方式从 $GF(p^r)$ 构造出来．

除上述定理中的有限准域外，蔡森豪斯证明恰好存在七个其他的准域．在这些情形里准域 K 的阶是 p^2，而且只要给出以加法群的两个生成元素的矩阵变换表出的乘法群 M 的生成元素．我们按照蔡森豪斯那样来编排次序．

I. $n=5^2$, $A=\begin{pmatrix}0, & -1\\ 1, & 0\end{pmatrix}$, $B=\begin{pmatrix}1, & -2\\ -1, & -2\end{pmatrix}$.

$$M\cong M(2,3).$$

II. $n=11^2$,

$$A=\begin{pmatrix}0, & -1\\ 1, & 0\end{pmatrix},\ B=\begin{pmatrix}1, & 5\\ -5, & -2\end{pmatrix},\ C=\begin{pmatrix}4, & 0\\ 0, & 4\end{pmatrix}.$$

$$M \cong M(2,3) \times (C).$$

III. $n = 7^2$, $A = \begin{pmatrix} 0, & -1 \\ 1, & 0 \end{pmatrix}$, $B = \begin{pmatrix} 1, & 3 \\ -1, & -2 \end{pmatrix}$.

$$M \cong G_3.$$

IV. $n = 23^2$, $A = \begin{pmatrix} 0, & -1 \\ 1, & 0 \end{pmatrix}$, $B = \begin{pmatrix} 1, & -6 \\ 12, & -2 \end{pmatrix}$,

$$C = \begin{pmatrix} 2, & 0 \\ 0, & 2 \end{pmatrix},$$

$$M \cong G_3 \times (C)$$

V. $n = 11^2$, $A = \begin{pmatrix} 0, & -1 \\ 1, & 0 \end{pmatrix}$, $B = \begin{pmatrix} 2, & 4 \\ 1, & -3 \end{pmatrix}$.

$$M \cong M(2,5).$$

VI. $n = 29^2$, $A = \begin{pmatrix} 0, & -1 \\ 1, & 0 \end{pmatrix}$, $B = \begin{pmatrix} 1, & -7 \\ -12, & -2 \end{pmatrix}$,

$$C = \begin{pmatrix} 16, & 0 \\ 0, & 16 \end{pmatrix}.$$

$$M \cong M(2,5) \times (C).$$

VII $n = 59^2$,

$$A = \begin{pmatrix} 0, & -1 \\ 1, & 0 \end{pmatrix},\ B = \begin{pmatrix} 9, & 15 \\ -10, & -10 \end{pmatrix},\ C = \begin{pmatrix} 4, & 0 \\ 0, & 4 \end{pmatrix}.$$

$$M \cong M(2,5) \times (C).$$

这里 $M(2,3)$ 是 I 中给出的 24 阶群；$M(2,5)$ 是 V 中给出的 120 阶群；G_3 是 III 中给出的 48 阶群．$M(2,5)$ 有 2 阶的中心 Z，而且商群 $M(2,5)/Z$ 是 60 阶的单纯群．

20.8. 有限平面．勃鲁克-累色尔定理

在 n 阶的有限平面上，我们曾证明下列性质成立：

1）存在 n^2+n+1 条线.

2）存在 n^2+n+1 个点.

3）每条线包含 $n+1$ 个点.

4）每个点在 $n+1$ 条线上.

5）存在唯一的线通过两个不同的点.

6）两条不同的线相交于唯一的点.

在验证一个体系是有限平面时，较方便的是先知道一下"点"和"线"的体系在具有上述性质的那一部分时就一定是 n 阶的有限平面而且具有其他的性质.

定理 20.8.1. 点和线的体系如果满足(1)，(3)和(5)或满足对偶的(2)，(4)和(6)，则它是 n 阶的有限平面而且具有其余的性质.

证明. 假定体系满足(1)，(3)和(5). 设点 P_i 在 m_i 条线上. 那么 P_i 就与 m_i 条线上各 n 个其他的点连接着. 而这些就是全部其余的点，而且每个点恰好计算一次，因此一共存在 $1+nm_i$ 个点. 因此 $m=m_i$ 对于每个点是相同的. 考虑点在线上的关联性，我们有

$$(n+1)(n^2+n+1)=m(1+mn).$$

因为存在着各包含 $n+1$ 个点的 n^2+n+1 条线和各在 m 条线上的 $1+mn$ 个点. 这给出 $m=n+1$，因而得出(2)和(4). 根据(5)，我们不能有两条不同的线相交于一个以上的点. 为了证明(6)，我们只需要证明，存在一个点是两条不同的线的交点. 已知线 L 上的点 P 在 n 条其他的线上，这对于 L 的 $n+1$ 个点中的每一个都成立. 因此 L 与 $n(n+1)=n^2+n$ 条其他的线相交，但是这是全部其余的线，所以(6)成立. 这证明了从(1)，(3)，(5)得出其余的性质. 用对偶的论证可以证明从(2)，(4)，(6)得出其余的性质.

推论 20.8.1. 在有限的韦勃伦-魏德本体系内，定理

20.4.6 的条件 (4)，即当 $r \neq s$ 时 $xr = xs + t$ 有唯一解，是其余条件的结果.

因为不利用条件 (4) 就能证明性质 (1), (3) 和 (5) 成立.

并不是对于每个整数阶 n 都存在有限平面. 如果欧拉的一个猜想成立，则当 $n \equiv 2 \pmod 4$, $n \neq 2$ 时，就不存在 n 阶的平面. 塔雷 (Tarry [1]) 在 1900 年用试错法证明，不存在 6 阶的平面. 对于每个素数方幂 $n = p^r$ 存在域 $GF(p^r)$，因而根据定理 20.5.5，存在 p^r 阶的德沙格平面，存在着除 4 阶以外的 p^{2r} 阶的赫尔体系，这产生非德沙格平面. 又准域也产生非德沙格平面. 对于奇素数 p 和 $r > 2$，阿尔贝特 (Albert [1]) 构造了 p^r 阶的非结合的可除环. 根据定理20.4.6，这当然就产生这个阶的非德沙格平面. 对于奇素数 p 和奇数 $r > 1$，我们给出阿尔贝特的一个简单构造.

定理 20.8.2 (阿尔贝特). 设 p 是奇素数，r 是奇数，$r > 1$. 那么从 $GF(p^r)$ 可以构造具有 p^r 个元素的非结合的可除代数 N.

证明. 对于奇素数 p，奇数 $r > 1$，我们用下列规则建立 $GF(p^r)$ 的元素的新的乘积 (x, y):

$$(x, y) = \frac{1}{2}(xy^p + x^p y). \qquad (20.8.1)$$

因为 $x \to x^p$ 是 $GF(p^r)$ 的自同构，所以容易验证乘积 (x, y) 满足分配律，我们希望证明，如果 $x \neq 0$, $y \neq 0$，则 $(x, y) \neq 0$. 假定相反地有 $x \neq 0$, $y \neq 0$ 而 $(x, y) = 0$. 那么我们有

$$xy^p = -x^p y, \qquad (20.8.2)$$

因而

$$y^{p-1} = -x^{p-1}. \qquad (20.8.3)$$

因为 r 和 p 都是奇数，$m = (p^r - 1)/(p - 1)$ 是奇数. 作

(20.8.3) 式两边的 m 次方幂，我们得出

$$1=y^{p^r-1}=-x^{p^r-1}=-1, \qquad (20.8.4)$$

因为 $p\neq 2$，这是一个矛盾．因此如果 $x\neq 0$，$y\neq 0$，则 $(x, y)\neq 0$． 因为我们的体系是有限的而且没有零因子，它必定是拟群．因而给定 $x\neq 0$，就存在唯一的 $u\neq 0$，使得

$$x=(u,\ 1)=\frac{1}{2}(u+u^p). \qquad (20.8.5)$$

因此当 u 和 x 满足 (20.8.5) 时，我们可以定义一一映射 α:

$$u=x\alpha. \qquad (20.8.6)$$

现在我们定义以 $GF(p^r)$ 的元素作为元素的体系 D，D 中的加法就是 $GF(p^r)$ 中的加法，但是 D 中的乘积 $x\circ y$ 由下式给出:

$$x\circ y=(x\alpha, y\alpha), \qquad (20.8.7)$$

这里用到 (20.8.1) 的乘积和 (20.8.6) 的映射． $GF(p^r)$ 中的单位元素是 D 中的单位元素，因为我们可以验证．

$$x\circ 1=1\circ x=x. \qquad (20.8.8)$$

D 中的乘法是交换的而不是结合的． 阿尔贝特曾证明，不在 F_p 内的一个元素的自乘就不是结合的．

这里所给的方法产生了 p^r 阶 ($r\geqslant 2$ 而且 p 是奇数) 和 2^r 阶 (r 是偶数而且 $r\geqslant 4$) 的非德沙格平面．已经证明只存在阶为 2, 3, 4, 5, 7, 8 的德沙格平面． 还知道有其他的有限平面，包括将在后面讨论的修格斯平面，但是已经构造出来的有限平面都是阶为素数或素数方幂的．

除去塔雷的不存在 6 阶平面的孤立结果以外，直到 1949 年还不知道关于平面的可能的阶的任何限制． 在 1949 年勃鲁克和累色尔 (Bruck and Ryser[1]) 证明了下列主要定理．

定理 20.8.3. 如果 $n\equiv 1, 2 \pmod 4$，则除非 n 可以表示成两个整数的平方和: $n=a^2+b^2$，不可能存在 n 阶平面．

证明. 这里所给的证明是从周拉和累色尔 (Chowla and Ryer [1]) 的方法对原来的证明作一些修改而成. 设 $N = n^2 + n + 1$. 设变数 x_i, $i = 1, \cdots, N$ 对应 n 阶平面 π 的点 P_i, $i = 1, \cdots, N$. 设 π 的线是 L_j, $j = 1, \cdots, N$. 我们定义关联数 a_{ij}:

$$a_{ij} = 1, \text{ 如果 } P_i \in L_j,$$
$$a_{ij} = 0, \text{ 如果 } P_i \notin L_j, \ i, j = 1, \cdots, N. \tag{20.8.9}$$

然后定义 π 的关联矩阵 A:

$$A = (a_{ij}), \ i, j = 1, \cdots, N. \tag{20.8.10}$$

这个关联矩阵满足基本的关系

$$AA^T = A^T A = nI + S, \tag{20.8.11}$$

这里 I 是单位矩阵而 S 是每个元素都是 1 的矩阵.

设 $AA^T = C$. 那么 $C = (c_{rs})$, 其中

$$c_{rs} = \sum_{j=1}^{N} a_{rj}\, a_{sj}. \tag{20.8.12}$$

这里 $c_{rr} = n + 1$, 因为 P_r 恰好在 $n + 1$ 条线上, 此因 a_{rj}, $j = 1, \cdots, N$, 恰好有 $n + 1$ 个 1, 其余都是 0. 又如果 $r \neq s$, 则我们有 $c_{rs} = 1$, 因为 $a_{rj}a_{sj} = 0$, 否则就会同时有 $a_{rj} = 1$ 和 $a_{sj} = 1$. 而 $a_{rj} = a_{sj} = 1$ 是说线 L_j 包含 P_r 和 P_s. 可是给定 P_r 和 P_s, 恰好存在一条线 L_j 包含这两个点. 因此 $c_{rr} = n + 1$, $c_{rs} = 1$, $r \neq s$, 所以 $AA^T = nI + S$. 用对偶的论证可以证明 $A^T A = nI + S$.

关系式 $AA^T = nI + S$ 也可以用二次齐式表出. 线 L_j 可以对应于线性齐式, 它也可以记做 L_j 而不引起混淆. 我们记

$$L_j = \sum_{i=1}^{N} a_{ij} x_i, \ j = 1, \cdots, N. \tag{20.8.13}$$

那么

$$L_1^2 + \cdots + L_N^2 = n(x_1^2 + \cdots + x_N^2) + (x_1 + \cdots + x_N)^2. \tag{20.8.14}$$

为此我们注意到，在 $L_j(j=1,\cdots,N)$ 内每个 x_r 以系数 1 而出现恰好有 $n+1$ 次，因为每个点在 $n+1$ 条线上.我们还注意到交叉乘积 $2x_rx_s$ 在 $L_1^2+\cdots+L_N^2$ 内恰好出现一次，因为恰好存在一条线 L_j 包含点 P_r 和 P_s. 这就证明了恒等式(20.8.14). 现在假定 $n\equiv 1, 2 \pmod 4$，那么 $N=n^2+n+1\equiv 3 \pmod 4$. 我们还看到(20.8.14)可以改写成:

$$L_1^2+\cdots+L_N^2=n\left(x_2+\frac{x_1}{n}\right)^2+\cdots$$

$$+n\left(x_N+\frac{x_1}{n}\right)^2+(x_2+\cdots+x_N)^2. \qquad (20.8.15)$$

考虑到在(20.8.15)的右边，x_1^2 的系数是 $(N-1)/n=n+1$，就能得出这个等式. 在(20.8.15)里更换变数，记

$$y_1=x_2+\cdots+x_N,\ y_2=x_2+\frac{x_1}{n},\cdots,$$

$$y_N=x_N+\frac{x_1}{N}. \qquad (20.8.16)$$

这时这些 x 可以用这些 y 的有理式表出. 我们把(20.8.15)改写成

$$L_1^2+\cdots+L_N^2=y_1^2+ny_2^2+ny_3^2+\cdots+ny_N^2. \qquad (20.8.17)$$

我们现在引用每个正整数可以表示成四个平方数之和的拉格朗日定理. 这可以参考哈代和雷特著的《数论》(Hardy and Wriht [1]) 第 300 页. 总之我们有

$$n=a_1^2+a_2^2+a_3^2+a_4^2, \qquad (20.8.18)$$

还有著名的拉格朗日恒等式

$$(a_1^2+a_2^2+a_3^2+a_4^2)(y_i^2+y_{i+1}^2+y_{i+2}^2+y_{i+3}^2)$$
$$=(a_1y_i+a_2y_{i+1}+a_3y_{i+2}+a_4y_{i+3})^2$$
$$+(a_1y_{i+1}-a_2y_i+a_3y_{i+3}-a_4y_{i+2})^2$$
$$+(a_1^2y_{i+2}-a_3y_i+a_4y_{i+1}-a_2y_{i+3})^2$$
$$+(a_1y_{i+3}-a_4y_i+a_2y_{i+2}-a_3y_{i+1})^2$$

$$= z_i^2 + z_{i+1}^2 + z_{i+2}^2 + z_{i+3}^2. \tag{20.8.19}$$

在(20.8.19)里 $z_i, z_{i+1}, z_{i+2}, z_{i+3}$ 由 $y_i, y_{i+1}, y_{i+2}, y_{i+3}$ 的有理式表出. 回想到 $N \equiv 3(\mathrm{mod}\ 4)$, 我们可以应用(20.8.18)和(20.8.19)到(20.8.17)而得出

$$L_1^2 + \cdots + L_N^2 = z_1^2 + z_2^2 + \cdots + z_{N-2}^2 + n(z_{N-1}^2 + z_N^2). \tag{20.8.20}$$

我们注意到每个 $L_j(j = 1, \cdots, N)$ 原来就是这些 x 的有理线性齐式(事实上是整线性齐式), 因而依次是 y 的和 z 的有理线性齐式,这里 $z_1, \cdots, z_N$ 是独立未知数. 因为(20.8.20)是关于 z 的恒等式, 所以当某些 z 特别成为其余 z 的线性组合时,它仍然成立. 假定在(20.8.20)里

$$L_1 = (b_1 z_1 + \cdots + b_N z_N). \tag{20.8.21}$$

当 $b_1 \neq 1$ 时我们令 $L_1 = z_1$, 当 $b_1 = 1$ 时令 $L_1 = -z_1$. 这就可以用来使 z_1 特殊成为 $z_2, \cdots, z_N$ 的有理线性组合而且给出 $L_1^2 = z_1^2$. 对于这个特殊的 z_1, 我们有

$$L_2^2 + \cdots + L_N^2 = z_2^2 + \cdots + z_{N-2}^2 + n(z_{N-1}^2 + z_N^2). \tag{20.8.22}$$

继续下去, 我们令 $L_2 = \pm z_2, \cdots, L_{N-2} = \pm z_{N-2}$ 来取特殊的 $z_2, \cdots, z_{N-2}$, 最后得出

$$L_{N-1}^2 + L_N^2 = n(z_{N-1}^2 + z_N^2), \tag{20.8.23}$$

这里 L_{N-1} 和 L_N 是 z_{N-1} 和 z_N 的有理线性齐式而且 z_{N-1} 和 z_N 是独立的未知数. 我们可以取 z_{N-1} 和 z_N 的这样的正整数值, 使它们都是 L_{N-1} 和 L_N 的系数的分母的倍数, 于是(20.8.23)就成为整数之间的一个关系式. 现在 n 是两个整数的商,而这两个整数又都是两个平方数的和,根据从哈代和雷特的书(Hardy and Wright [1])上定理 366 得出的数论的一个熟知结论, n 本身也是两个平方数的和. 总之,

$$n = a^2 + b^2, \tag{20.8.24}$$

我们的定理也就证明了．这个定理有一个部分的逆命题：

定理 20.8.4. 如果 $n \equiv 0, 3 \pmod 4$ 或如果 $n \equiv 1, 2 \pmod 4$ 而 $n = a^2 + b^2$，则就存在 $x_1, \cdots, x_N$ 的有理线性齐式 $L_j, j = 1, \cdots, N$，满足

$$L_1^2 + \cdots + L_N^2 = n(x_1^2 + \cdots + x_N^2) + (x_1 + \cdots + x_N)^2.$$

还存在 $N \times N$ 矩阵 A 满足 $AA^T = A^TA = nI + S$.

证明. 如果 $n \equiv 0, 3 \pmod 4$，则我们可以利用(20.8.18)和(20.8.19)而把(20.8.17)变成：

$$L_1^2 + \cdots + L_N^2 = z_1^2 + \cdots + z_N^2, \qquad (20.8.25)$$

当然 $L_i = z_i$ 就满足定理的要求．如果 $n = 1, 2 \pmod 4$ 而且 $n = a^2 + b^2$，我们可以利用恒等式

$$(a^2 + b^2)(y_i^2 + y_{i+1}^2) = (ay_i + by_{i+1})^2 + (by_i - ay_{i+1})^2 = z_i^2 + z_{i+1}^2 \qquad (20.8.26)$$

代替(20.8.19)而使(20.8.17)成为(20.8.25)的形状．如果

$$L_j = \sum_i b_{ij}x_i, \; j = 1, \cdots, N \qquad (20.8.27)$$

是定理中的线性齐式，则令 $A = (b_{ij}), i, j = 1, \cdots, N$，就有

$$AA^T = nI + S, \qquad (20.8.28)$$

但是一般并没有 $A^TA = nI + S$．要证明在定理的假设下存在有理矩阵 A 同时满足关系 $AA^T = nI + S = A^TA$ 是相当困难的．但是赫尔和累色尔(Hall and Ryser[1])证明了比这还多的结果．

20.9. 有限平面的直射

如果平面 π 的直射 α 不变两个点，则它也不变它们的连线，同理，如果它不变两条线，则它也不变它们的交点．因此，如果 α 不变一个四点形，则 α 不变 π 的一个真子平面．下列

定理给出关于子平面的可能的阶的知识.

定理 20.9.1（**勃鲁克**）. 如果 n 阶平面 π 有 m 阶的子平面 π^*，则 $n = m^2$ 或 $n \geqslant m^2 + m$.

证明. 设 L 是子平面 π^* 的线而 P 是 L 上不属于 π^* 的点. 存在 π^* 的在 L 上的 $m + 1$ 个点和不在 L 上的 m^2 个点. 连结 P 与 π^* 的不在 L 上的 m^2 个点的每一个，我们得到通过 P 的 m^2 条线，它们必定都不相同，因为如果有两条相同的，则这样的线 K 就会包含 π^* 的两个不同的点，因而它是 π^* 的线，于是 P 作为 K 和 L 的交点就将是 π^* 的点而与假设矛盾. 因此至少存在 $m^2 + 1$ 条通过 P 的线，那就是 L 和连结 P 与 π^* 的点的其他 m^2 条线. 于是因为存在 $n + 1$ 条通过 P 的线，所以 $n \geqslant m^2$. 如果 $n \neq m^2$，则就存在通过 P 而不通过 π^* 的点的线 L_1. 考虑 L_1 与 π^* 的 $m^2 + m + 1$ 条线的交点. 如果这种交点中有任何两个是相同的点，则这个点将是 π^* 的点而与假设矛盾. 因此 L_1 至少包含 $m^2 + m + 1$ 个点，所以 $n \geqslant m^2 + m$.

稍加注意就能列出平面的这种子集 S，它在包含两个点的同时还包含它们的连线，又在包含两条线的同时还包含它们的交点.

首先，如果 S 包含没有三个共线的四个点，则 S 是一个子平面. 剩下的可能集合我们叫做退化的子平面. 这些是:

1）空集.

2）单独一个点 P，而且可以带上通过 P 的一条或更多的线.

3）单独一条线 L，而且可以带上在 L 上的一个或更多的点.

4）单独一个点 P 和通过 P 的单独一条线 L.

5）一个三角形的三个顶点和三条边.

6）线 L 和 L 上的点 P，再有 L 上的一个或更多的点以及通过 P 的一条或更多的线.

7）线 L 和 L 上的三个或更多的点，不在 L 上的点 P 以及 P 和 L 上的点的连线.

直射 α 是 π 的点的置换也是 π 的线的置换. 设 P 是点的置换，Q 是线的置换，我们可以把 P 和 Q 都记做 $N\times N$ 矩阵，这里仍然设 $N=n^2+n+1$.

$$P=(p_{ij}),\quad Q=(q_{ij}), \tag{20.9.1}$$

这里 $p_{ij}=1$，如果 $P_i\alpha=P_j$，

$q_{ij}=1$，如果 $Q_i\alpha=Q_j$，

否则 $p_{ij}=0$，$q_{ij}=0$.

于是我们有

$$P^{-1}AQ=A, \tag{20.9.2}$$

这里 $A=(a_{ij})$ 是 π 的关联矩阵. 反之，如果存在置换矩阵 P 和 Q 满足 (20.9.2)，则它们决定 π 的一个直射.

定理 20.9.2（帕克尔[1]）. 在直射下的点置换 P 和线置换 Q 作为置换是相似的.

推论 20.9.1（白尔）. 在直射下不变的点和线的个数相同.

证明. 我们注意到，因为

$$AA^T=A^TA=nI+S, \tag{20.9.3}$$

所以

$$(\det A)^2=\det(nI+S)=(n+1)^2n^{N-1}, \tag{20.9.4}$$

因而 A 是可逆的. 因此 (20.9.2) 变成

$$Q=A^{-1}PA, \tag{20.9.5}$$

所以 P 和 Q 作为矩阵是相似的. 这里 P 和 Q 具有作为循环群

1）参看 Parker[1].

的表示的相同的不可约传递组．但是在任何置换里简化长度为 r 的圈 $(x_1, \cdots, x_r)$ 时，我们发现这些传递组具有特征标 $1, \zeta, \zeta^2, \cdots, \zeta^{r-1}$，这里 ζ 是 r 次本原单位根．而这说明有一个 m 次单位根是具有乘数 a_m 的置换 P 的特征标，这里 a_m 是 P 中长度为 m 的倍数的圈的个数．因为这些乘数 a_m 对于 P 和 Q 是相同的，所以 P 和 Q 所具有的每一长度 m 的圈的个数都相同．因此 P 和 Q 作为置换是相似的．特别还得出推论，它断定 P 和 Q 所具有的长度为一的圈（即不变元素）的个数相同．

定理 20.9.3（帕克尔）． π 的直射群 G 作为点上的置换群和作为线上的置换群具有相同个数的传递组．

证明． 设 G 的阶是 g，那么根据 (20.9.5)，我们可以把 G 表成点上的置换群 G_1 和线上的置换群 G_2，而且这两个表示是等价的．设 χ_1 和 χ_2 分别是它们的特征标：

$$\sum_{x \in G} \chi_1(x) = \sum_{x \in G} \chi_2(x). \qquad (20.9.6)$$

但是根据定理 16.6.13，

$$\sum_{x \in G} \chi_1(x) = k_1 g, \quad \sum_{x \in G} \chi_2(x) = k_2 g, \qquad (20.9.7)$$

这里 k_1 是 G 的传递组数，k_2 是 G_2 的传递组数．因此 $k_1 = k_2$，这就是定理的结论．虽然从前面一个定理，G_1 的每个置换作为置换而与 G_2 的对应元素相似，但是一般说来 G_1 和 G_2 作为置换群并不一定相似．举例说，在德沙格平面上，不变一个点 P_0 的全体直射的群并不包含被它的全体直射都不变的线．

定理 20.9.4． 阶为 $n = p^r$ 的德沙格平面 π 具有阶为

$$r(n^2 + n + 1)(n^2 + n)n^2(n - 1)^2$$

的直射群．

证明． 在 π 上的有序四点形 P_1, P_2, P_3, P_4 的个数是

$$(n^2+n+1)(n^2+n)n^2(n-1)^2,$$

因为我们可以取 n^2+n+1 个点中的任何一个作为 P_1，取任何别一个作为 P_2，取不在 P_1P_2 上的 n^2 个点中的任何一个作为 P_3，取不在 P_1P_2, P_1P_3 和 P_2P_3 上的 $(n-1)^2$ 个点中的任何一个作为 P_4. 根据定理 20.5.5，π 的直射群 G 在四点形上是传递的，G 的不变四点形 X, Y, O, I 的子群是坐标域 $GF(p^r)$ 的自同构群，在§ 20.6 中曾指出过它的阶是 r.

定理 20.9.5 (**辛格尔**[1]). 阶为 n 的德沙格平面 π 具有阶为 $N=n^2+n+1$ 的直射 α，它循环置换 π 的全体点和线.

证明. 设 $n=p^r$. 那么 π 可以用 $GF(p^r)=F$ 建立坐标. 适宜于用齐次坐标来表示 π. 点 P 可以记做

$$P=(\lambda x_1, \lambda x_2, \lambda x_3), \tag{20.9.8}$$

这里 x_1, x_2, x_3 是 F 的不全是零的定元素，而 λ 可以取 F 的除 0 外的所有元素. 同理，线 L 可以记做

$$L=[u_1\mu, u_2\mu, u_3\mu], \tag{20.9.9}$$

这里 u_1, u_2, u_3 是 F 的不全是零的定元素，而 μ 可以取 F 的除 0 外的所有元素. $P\in L$，必要而且只要

$$x_1u_1+x_2u_2+x_3u_3=0. \tag{20.9.10}$$

因为 F 是域，所以关联关系 (20.9.10) 对于 (20.9.5) 中的任何 λ 和 (20.9.9) 中的任何 μ 都是一样的. 齐次坐标可以用下列方式与非齐次坐标等同起来:

$$\begin{aligned}(\infty)&=(0, \lambda, 0),\\ (m)&=(\lambda, \lambda m, 0),\\ (a, b)&=(\lambda a, \lambda b, \lambda),\\ L_\infty&=[0, 0, \mu].\\ (x=c)&=[\mu, 0, -c\mu],\end{aligned} \tag{20.9.11}$$

1) 参看 Singer[1].

$$(y = xm + b) = [m\mu, \ -\mu, b\mu].$$

我们容易验证 π 的齐次表示与非齐次表示是协调的. 域 $GF(p^{3r}) = F_1$ 可以看做是 $F = GF(p^r)$ 的三次扩张，而且如果 w 是 F_1 的一个本原根，则 F_1 的每个元素 x 有唯一的表示

$$x = x_1 + x_2 w + x_3 w^2, \ x_i \in F. \tag{20.9.12}$$

因此，如果 $x \neq 0$，$\lambda \in F$，$\lambda \neq 0$，则 F_1 的元素 λx 对应于 π 的点 $(\lambda x_1, \lambda x_2, \lambda x_3)$. 但是在 F_1 内，w 的阶是 $p^{3r} - 1 = n^3 - 1$. F 的元素是 F_1 中的方程

$$x^{p^r} = x \tag{20.9.13}$$

的解，因而对于 $x \in F$，$x \neq 0$，由于 $n = p^r$，我们有

$$x^{n-1} = 1. \tag{20.9.14}$$

于是 F^* (F 的非 0 元素的集合)是阶为 $n^3 - 1$ 的循环群 $\{w\}$ 的唯一的 $n - 1$ 阶子群. 因此 F^* 的元素是

$$w^{Ni}, \ N = n^2 + n + 1. \tag{20.9.15}$$

因而 w^u 和 w^v 表示 π 的同一个点，必要而且只要

$$u \equiv v (\mathrm{mod} N), \tag{20.9.16}$$

因此元素 $x \in F_1$ 的映射 α:

$$x \to xw \tag{20.9.17}$$

作为 π 的点的置换是长度 N 的圈. 如果 $P_1 = (x_1, x_2, x_3)$ 和 $P_2 = (y_1, y_2, y_3)$ 是两个不同的点，则我们容易验证线 P_1P_2 的点可以表成

$$\begin{aligned} &\lambda_1(x_1, x_2, x_3) + \lambda_2(y_1, y_2, y_3) \\ &= (\lambda_1 x_1 + \lambda_2 y_1, \lambda_1 x_2 + \lambda_2 y_2, \lambda_1 x_3 + \lambda_2 y_3), \end{aligned} \tag{20.9.18}$$

这里 λ_1 和 λ_2 是 F 中不全是零的任意元素，因此，如果 $w^i = x_1 + x_2 w + x_3 w^2$，$w^j = y_1 + y_2 w + y_2 w^2$，则 P_1P_2 的点可以表成

$$\lambda_1 w^i + \lambda_2 w^j. \tag{20.9.19}$$

因此，映射 $x \to xw$ 把由 (20.9.19) 表出的点变成

$$\lambda_1 w^{i+1} + \lambda_2 w^{j+1}, \tag{20.9.20}$$

这些都是$P_1\alpha$和$P_2\alpha$的连线的点. 因此α是π的直射而且是点上的长度为N的圈. 容易发现(例如根据定理 20.9.2)α也是π的线上的长度为N的圈.

我们可以给出n阶平面π的直射群G的阶的一个粗糙的上界. 有序四点形P_1, P_2, P_3, P_4最多有$M=(n^2+n+1)\times(n^2+n)n^2(n-1)^2$个像. 指数$\leqslant M$的不变$P_1, P_2, P_3, P_4$的子群$H_1$不变由这些点生成的子平面$\pi_1$. 如果$\pi_1$是$m_1$阶的, 则$H_1$置换$\pi_1$的线上不属于$\pi_1$的$n-m_1$个点. H_1中不变一个这种点的指数$\leqslant n-m_1$的子群H_2, 不变阶为m_2的较大的子平面π_2,根据定理 20.9.2, $m_2\geqslant m_1^2$.因而我们有子群的递降序列$H_1\supset H_2\supset\cdots\supset H_s=1$, 这里$H_i$不变阶为$m_i$的子平面,这里$m_{i+1}\geqslant m_i^2$而且$[H_i:H_{i+1}]<n$. 因而$s\leqslant\log_2 n$, 而且$G$的阶最多是$n^sM$. 熟知的一些非德沙格平面的直射群没有象同阶的德沙格平面的直射群那么大, 看来好象总是出现这样的情况.

下面两个定理断定, 如果有限平面的直射群在某种特殊的方式下是充分大的,则这平面是德沙格平面.

定理 20.9.6 (格列逊[1]). 如果对于P是有限平面π的线L上的点的每一对P和L, 合射群$G(P, L)$不是单位元素群, 则π是德沙格平面.

证明. 根据定理 20.4.3, 如果对于L的不同的点P_1和P_2,合射群$G(P_1,L)$和$G(P_2,L)$不是单位元素群,则以L为轴的全体合射组成阿贝尔群, 其中每个$\neq 1$的元素有相同的阶p, 根据这个定理的对偶,如果$G(P, L_1)$和$G(P, L_2)$不是单位元素群,这里L_1和L_2是通过P的不同的线,则以P为中心的全体合射组成阿贝尔群, 它的$\neq 1$的元素有相同的素数阶

---

1) 参看 Gleason[1].

p. 因此，在本定理的假设下，每个合射群 $G(P, L)$是阶为 p 或 p 的方幂的初等阿贝尔群.

引理 20.9.1. 假定H是有限集合 S 的置换群，而且对于某个 p 和每个 $x\in S$，存在H的 p 阶元素，它不变 x 而变动 S 的其他元素. 那么H是传递的.

证明. 设 S_1 是 S 在H下的传递组. 对于 $x\in S_1$，存在 p 阶元素不变 x 而且以长度 p 的圈而变动全体其余的元素. 因此 S_1 中元素的个数与 1 同余 (mod$p$)，而且在另一个传递组 S_2(如果存在的话) 中元素的个数是 p 的倍数. 于是取 $y\in S_2$ 而运用同样的论证,就得出S_1中元素的个数也是 p 的倍数.这是一个矛盾,因而只存在一个传递组而且H在 S 上是传递的.

引理 20.9.2. 假定对于有限平面 π 的线 L，合射群 $G(P_i, L)$ 对于所有 $P_i\in L$ 具有相同的阶 $h>1$. 那么π是相对于L的平移平面.

证明. 设π的阶是n. $n+1$ 个 h 阶群 $G(P_i, L)$ 中的任何两个只有单位元素群是公共的，而且它们的元素共同组成平移群 $T(L)$. 因此 $T(L)$ 的阶是 $t=(n+1)(h-1)+1$. 因此只有 $T(L)$ 的单位元素群才能不变不在L上的点，$T(L)$ 以 t 个点为一组而置换那 n^2 个点,因而 t 整除 n^2. 记

$$n^2=tm=[(n+1)(h-1)+1]m. \qquad (20.9.21)$$

因为 $h>1$, 我们有 $m<n$, 另一方面, (20.9.21) 取模 $n+1$, 我们有

$$n^2\equiv 1\equiv m(\bmod n+1). \qquad (20.9.22)$$

然而 $m\equiv 1(\bmod n+1)$ 和 $m<n$ 共同推出 $m=1$, $t=n^2$, 因而 $T(L)$ 在π的不在L上的 n^2 个点上是传递的，所以π是相对于L的平移平面.

现在可以来证明我们的定理了. 取π的一条固定的线 L. 对于每个点 $P\in L$ 和通过P的另一条线 $M\neq L$，合射群

$G(P, M)$ 包含不变 P 的 p 阶元素，它把 L 变到自身但是变动 L 的所有其他的点. 因此根据引理 20.9.1，不变 L 的全体直射的群 $G(L)$ 在 L 的点上是传递的. 于是由此得出，对于 L 的 $n+1$ 个点 P_i，在 $G(L)$ 下共轭的全体合射群 $G(P_i, L)$ 具有相同的阶 h. 根据引理 20.9.2，由此得出 π 是相对于 L 的平移平面. 但是 L 可以取 π 的任意的线. 因而 π 是相对于每一条线 L 的平移平面，于是根据定理 20.5.3，π 可以取一个交替可除环来建立坐标. 根据定理 20.6.2，有限交替可除环是域，因而 π 是德沙格平面.

格列逊 (Greason[1]) 在研究有限的法诺平面时用到这个定理. 法诺巧图是由七个点和七条线组成的图形，这使有限平面的阶是 2. 平面是法诺平面，假如每个四点形的对角点在一条线上，或者说每个四点形产生一个法诺巧图. 格列逊证明每个有限的法诺平面是德沙格平面，而且它们是域 $GF(r^2)$ 上的有限平面. 在这里不预备证明这个十分有趣的结果了.

我们把 2 阶的直射叫做对合.

定理 20.9.7 (白尔). 设 α 是阶为 n 的射影平面的对合. 那么或者 (1) $n = m^2$ 而且 α 的不变的点和线组成阶为 m 的子平面，或者 (2) α 是中心直射. 在情形 (2) 里，如果 n 是奇数，则 α 是透射，又如果 n 是偶数，则 α 是合射.

证明. 我们先证明每个点总在一条不变线上. 如果 P 不是不变点，则 $P\alpha \neq P$ 而且 α 不变动线 $PP\alpha$，它就是通过 P 的不变线. 如果 P 是不变点，连结 P 和另一个点 Q. 可能 $L = PQ$ 是不变线. 如果不这样，则 $Q\alpha \neq Q$ 而且 $Q\alpha \notin PQ$. 这时 $L\alpha = PQ\alpha$. 于是如果 R 是 L 上的第三个点，则 $R\alpha \in L\alpha$. 于是 α 交换线 $Q\alpha R$ 和 $QR\alpha$，因而它们的交点 S 是与 P 不同的另一个不变点. 这时候 PS 就是通过 P 的不变线. 根据对偶的论证，每一条线通过一个不变点.

连结一对不变点的线是不变线，两条不变线的交点是不变点．因此如果存在四个不变点，其中没有三个共线，则 α 的不变元素就组成 π 的真子平面 π_1．假定有的是这种情形而且 π_1 的阶是 m． 那么根据定理 20.9.1，$n \geqslant m^2$，而且根据这个定理的证明，我们发现在 $n > m^2$ 时，存在 π 的线不通过 π_1 的任何点．然而我们已经证明 π 的每条线都包含不变点．因此不能有 $n > m^2$，所以 $n = m^2$．这证明了定理的可能情形 (1).

现在假定不存在任何三个都不共线的四个不变点．那么不变点的图形将是怎样的呢？我们先证明存在包含三个不变点的线．设线 L_1 包含不变点 P_1．取不通过 P_1 的线 L_2．那么 L_2 包含不变点 $P_2 \neq P_1$． 我们现在有两个不变点 P_1 和 P_2，它们的连线 L 是不变线． 在 L 上取第三个点 Q．如果 Q 不变，则 L 就是所求的线．如果 Q 不是不变点，通过 Q 的线 L_3 包含不在 L 上的不变点 P_3．现在我们有了由不变点组成的三角形 P_1, P_2, P_3． 考虑不通过 P_1, P_2, P_3 中任何一个点的线 L_4． L_4 包含不变点 P_4，如果 P_4 不在线 P_1P_2, P_1P_3, P_2P_3 中的任何一条上，则 P_1, P_2, P_3, P_4 是四个不变点，没有三个共线，这是已经讨论过的第一种情形．因此 P_4 在这些线中的一条上，因而存在包含三个不变点的线．

现在有了包含三个不变点 $P_1P_2P_3$ 的线 L． 如果存在两个不在 L 上的点，则就有了不变点的四点形，这就是第一种可能情形．因此或者只存在一个不在 L 上的不变点，或者不存在．现在考虑任何点 $P_i \in L$． 存在通过 P_i 而且与 L 不同的线 K，而且当存在不在 L 上的点 P 时，K 与 PP_i 也不同．K 包含一个不变点．但是根据我们的选取，没有不在 L 上的不变点． 因此，在 K 上的不变点只能是 P_i．由此得出 L 的每个点 P_i 都是不变点． 因为 α 不变 L 的每个点，所以 α 是以 L 为轴的中心

直射，这是第二种可能情形的论断．存在着 π 的 n^2 个点不在 L 上，而且 α 的阶是 2．因此如果 n 是奇数，则 α 不变一个不在 L 上的点，所以它是透射．如果 n 是偶数，则 α 不变偶数个不在 L 上的点，因而当它有不变点时至少就要有两个．因此在现在这个情形，α 不能不变任何不在 L 上的点，所以它是合射．这就完成了定理的各部分的证明．

下列定理是奥斯特朗（Ostrom [1]）的一个定理的改进，此外他假定了 n 是奇数．

定理 20.9.8（奥斯特朗）． 如果当 n 不是平方数时，阶为 n 的有限射影平面 π 的直射群在 π 的点上是二重传递的，则 π 是德沙格平面．

证明． 设 G 是 π 的直射群．根据假设，G 在 π 的 $N = n^2 + n + 1$ 个点上是二重传递的．因为 $N(N-1)$ 整除 G 的阶，G 必定包含 2 阶元素，它是一个对合 α．因为 n 不是平方数，根据定理 20.9.7，由此得出当 n 是偶数时 α 是合射，而当 n 是奇数时 α 是透射．

引理 20.9.3． 在 G 内存在合射．

证明． 如果 n 是偶数，则对合 α 是合射．因此我们只需要考虑 n 是奇数的情形．考虑对合 α，它是透射，设它的中心是 P，轴是 L．设 A 是 L 的点而且 $A_1 \neq P$ 是不在 L 上的点．那么在 G 内存在元素 σ 把 P 变成 P 而且把 A 变成 A_1，于是 $\beta = \sigma^{-1}\alpha\sigma$ 是对合，它的中心是 P，它的轴 K 通过 A_1，因而与 L 不同．于是 $\alpha\beta$ 是中心直射，因为它不变所有通过 P 的线．如果 $\rho = \alpha\beta$ 不变不通过 P 的任何线 T，令 $T_1 = T\alpha$．那么 β 必定也交换 T 和 T_1，又如果 $T \neq T_1$，则 ρ 必定同时不变 T 和 T_1，因而根据定理 20.4.1；$\rho = 1$ 而且 $\alpha = \beta$，这是矛盾，因为 α 和 β 是具有不同的轴的对合．但是如果 $T = T_1$，则 T 是 α 的轴而且也是 β 的轴，又是矛盾，因为 α 和 β 有不同的

轴. 因此 ρ 不会不变不通过 P 的线，所以 ρ 是合射. 这就证明了引理.

我们现在可以考虑具有中心 P 在轴 L 上的合射 ρ. 设 P_i 是 L 的任何别的点. 那么在 G 内存在元素 σ 交换 P 和 P_i. 于是 σ 不变 L. 因此不变 L 的直射的群 $G(L)$ 在 L 的点上是传递的，因而对于 L 的全体点 P_i，合射群 $G(P_i, L)$ 具有同一个阶 h，而且 $h>1$，因为存在具有中心 P 在 L 上的合射 ρ. 根据定理 20.9.6 的引理 20.9.2，π 是相对于轴 L 的平移平面. 但是因为 G 在点上是二重传递的，L 的任何两个点可以被 G 的适当的元素映到任何别的线 K 的两个点. 因此 π 也是相对于 K 的平移平面，因而它是茂芳平面. 然而在证明定理 20.9.6 时曾经指出过，这说明 π 是德沙格平面. 瓦格纳 (A. Wagner) 的一篇未发表的文章证明，定理 20.9.8 对于不加限制的 n 也成立.

修格斯 (D. R. Hughes[3]) 提出平面的关联矩阵的一种推广. 设给了平面 π 和 π 的直射的群 G，这种矩阵的元素是 G 的群环 G^* 的元素，G^* 取整系数或在特征不整除 G 的阶的任何域里取系数. 可以得到关联方程 (20.9.3) 的同类物. 从定理 20.9.3，我们回忆在 G 下的传递线组的个数是与传递点组的个数相同的，我们把这个数记做 w，而且引进下列记号：

π，已知的阶为 π 的射影平面.

G，π 的阶为 g 的直射群.

P_i. $i=1, \cdots, w$，第 i 个传递点组的固定代表.

L_j，$j=1, \cdots, w$，第 j 个传递线组的固定代表.

H_i，G 的阶为 h_i 的不变 P_i 的子群.

T_j，G 的阶为 t_j 的不变 L_j 的子群.

$D_{ij}=\{x \mid x \in G, P_i x \in L_j\}$，$G$ 的 d_{ij} 个元素的集合.

$$\delta_{ij} = \sum x, \quad x \in D_{ij}. \tag{20.9.23}$$

$\delta_{ij}^* = \sum x^{-1}, \quad x \in D_{ij}.$

$D = (\delta_{ij}), i, j = 1, \cdots, w$, G^*上的矩阵.

$D' = (\delta_{ij}^*)^T, i, j = 1, \cdots, w$, G^* 上的矩阵.

$\rho_i = \sum x, x \in H_i, i = 1, \cdots, w.$

$\tau_j = \sum x, x \in T_j, j = 1, \cdots, w.$

$\gamma = \sum x, x \in G.$

S = 每个元素都是γ的 $w \times w$ 矩阵.

我们还用到几个对角矩阵:

$$C_1 = \operatorname{diag}(h_1^{-1}, h_2^{-1} \cdots, h_w^{-1}). \tag{20.9.24}$$

$C_2 = \operatorname{diag}(t_1^{-1}, t_2^{-1}, \cdots, t_w^{-1}).$

$P = \operatorname{diag}(\rho_1, \rho_2, \cdots, \rho_w).$

$L = \operatorname{diag}(\tau_1, \tau_2, \cdots, \tau_w).$

我们发现G中使$P_ix \in L_j$的元素x的集合D_{ij}的情况完全决定了π上的关联关系，因为π的每个点可以写成具有某个$i = 1, \cdots, w$和某个$u \in G$的P_iu，同理，每条线有形状L_jv. 其次，$P_iu \in L_jv$，必要而且只要$P_iuv^{-1} \in L_j$或$uv^{-1} \in D_{ij}$. 因此D的情况完全决定了π. 如果G只包含单位元素，我们看到D就是π的关联矩阵.

定理 20.9.9. 给了阶为n的平面π和π的阶为g的直射群G. 直射矩阵D满足下列关系:

$$DC_2D' = nP + S, \tag{20.9.25}$$

$$D'C_1D = nL + S,$$

$$DC_2S = (n+1)S,$$

$$SC_1D = (n+1)S.$$

证明. 为了证明第一个等式，我们来计算$U = DC_2D'$的元素，先计算主对角线上的元素，再计算主对角线外的元素. 如果$U = (u_{r,s}), r, s = 1, \cdots, w$，则我们先有

$$u_{rr} = \sum_{j=1}^{w} \frac{\delta_{rj}\delta_{rj}^*}{t_j}. \qquad (20.9.26)$$

在(20.9.26)内,单独一个 j 的项是

$$\sum \frac{xy^{-1}}{t_j}, \ x \in D_{rj}, \ y \in D_{rj}. \qquad (20.9.27)$$

我们看到对于 $x \in D_{rj}$, 整个傍系 $H_r x T_j$ 包含在 D_{rj} 内. 我们考虑 H_r 在 G 内的左傍系:

$$G = H_r + H_r x_2 + \cdots + H_r x v_r, \ v_r h_r = g. \ (20.9.28)$$

对于 $h \in H_r$, 具有 $x, y \in D_{rj}$ 的方程 $xy^{-1} = h$ 或 $x = hy$ 对于每个 $y \in D_{rj}$ 和一个适当的 $x \in D_{rj}$ 成立,因为 $H_r y \subseteq D_{rj}$, 因此对于给定的 $h \in H_r$, 有着 d_{rj} 个选择 $x_1 y \in D_{rj}$, 使得 $xy^{-1} = h$. 因此在(20.9.26)中 h 的系数是 $\sum_j d_{rj}/t_j$. 但是 d_{rj} 是使 $P_r x \in L_j$ 或 $P_r \in L_j x^{-1}$ 的 x 的个数. 对于 $x \in D_{rj}$, 在集合 $L_j x^{-1}$ 中的不同的线的个数是 d_{rj}/t_j. 但是 P_r 一共在 $n+1$ 条线上. 因此

$$\sum_j \frac{d_{rj}}{t_j} = n + 1. \qquad (20.9.29)$$

因此在(20.9.26)中 $h \in H_r$ 的系数是 $n+1$.

现在来考虑方程 $xy^{-1} = z$, $z \notin H_r$, 这时 P_r 和 $P_r z$ 是不同的点因而属于唯一的线 $L_m v$, 这里 m 和傍系 $T_m v$ 是唯一确定的. 如果对于某个 j 同时有 $x \in D_{rj}$, $y \in D_{rj}$, 则 $P_r y$ 和 $P_r z y = P_r x$ 都属于 $L_m v y$. 但是 $P_r y \in L_j$, $P_r x \in L_j$, 而且 $P_r x \neq P_r y$. 因此 $L_m v y = L_j$, 因而必须有 $j = m$, $vy \in T_m$. 于是在(20.9.26)中元素 z 只在 $j = m$ 的一项中出现,而且这时对于 $x, y \in D_{rm}$, 我们有 $xy^{-1} = z$ 对于每个 $y \in D_{rm}$ 都成立. 因而 $L_m y^{-1} = L_m v = P_r P_r z$ 而且由 $x = zy$ 决定一个 $x \in D_{rm}$. 但是这种 y 使得 y^{-1} 在傍系 $T_m v$ 内,它们恰好有 t_m 个. 因此在(20.9.26)中

z 的系数是 $t_m/t_m = 1$. 总之在(20.9.26)中，$h \in H_r$ 的系数是 $n+1$ 而且 $z \in H_r$ 的系数是 1. 因此我们证明了，(20.9.25)的第一个等式在主对角线上是成立的. 对于 $U = DC_2D'$ 中主对角线外的项，我们有

$$u_{rs} = \sum_{j=1}^{w} \frac{\delta_{rj}\delta_{sj}^*}{t_j}, \tag{20.9.30}$$

而对于单独一个 j 的项是

$$\sum \frac{xy^{-1}}{t_j}, \ x \in D_{rj}, \ y \in D_{sj}. \tag{20.9.31}$$

这时对于任何 $z \in G$，点 $P_r z$ 和 P_s 是不同的，因而属于唯一的线 $L_m v$，这里 m 和傍系 $T_m v$ 是唯一确定的. 于是如果 $xy^{-1} = z$，这里对于某个 j，$x \in D_{rj}$，$y \in D_{sj}$，则 $P_r x = P_r zy$ 和 $P_s y$ 在线 $L_m vy$ 上. 但是 $P_r x \neq P_r y$ 都在线 L_j 上. 因此 $L_m vy = L_j$，因而 $j = m$ 而且 $L_j y^{-1} = L_m v = P_s P_r z$. 但是这些 y 使得 y^{-1} 是 $T_m v$ 的元素而且它们共有 t_m 个. 又对于每个 $y^{-1} \in T_m v$，$L_m vy = L_m$ 和 $P_r zy \in L_m$，因而 $x = zy \in D_{rm}$. 因此在 u_{rs} 中的任何 z 的系数都简化成 t_m/t_m，所以 $u_{rs} = \sum_z$，$z \in G$，$u_{rs} = \gamma$，这就完成了(20.9.25)中第一个关系的证明.

(20.9.25)中第二个关系是第一个关系的对偶，因而它可以用同样的方式来证明.

在计算 $DC_2S = V = (v_{rs})$ 时，我们发现

$$v_{rs} = \sum_j \frac{\delta_{rj}}{t_j} \gamma = \sum_j \frac{d_{rj}}{t_j} \gamma, \tag{20.9.32}$$

但是根据(20.9.29)，这是 $(n+1)\gamma$. 这就证明了第三个关系，而第四个关系是对偶的，因而可以用同样的方式证明.

修格斯从关系(20.9.25)出发，得到了类似于勃鲁克-累色尔定理的限制那样的关于平面上可能有的直射的限制. 象勃鲁克-累色尔定理的原有证明一样. 这结果的证明用到赫

赛-闵可夫斯基关于二次齐式有理等价的深入结果,修格斯特别得出下列结论:

定理 20.9.10(**修格斯**). 设 π 是阶为 n 的平面,这时 n 满足勃鲁克-累色尔条件. 设 G 是 π 的阶为奇素数 p 的直射群. 设不变点的个数 u 是偶数. 那么这种直射存在的必要条件是: 方程:

$$x^2 = ny^2 + (-1)^{(p-1)/2}pz^2$$

有不全是零的整数解 x, y, z.

对于奇数阶 g (代替 p) 的直射群 G, 如果 G 的每个 $\neq 1$ 的元素都变动同一些点,则同样的结果成立.

修格斯定理象勃鲁克-累色尔定理一样,否定了某些直射的存在,而并不是保证满足条件的直射的存在.

下列定理的主要内容是: 如果平面 π 有某个直射群 G, 则 π 必定还有一些特殊的直射. 我们假定 G 是简单类型的. 明白地说,我们将假定 G 在 π 的 $N = n^2 + n + 1$ 个点上是传递的和正则的,而且 G 还是阿贝尔群. 在 G 是循环作用在 π 的 N 个点上的 N 阶群的情形,这个结果最初由赫尔 (Hall [3]) 证明. 勃鲁克 (Bruck [1]) 推广而研究 G 是传递的和正则的情形, 但是还假定 G 是阿贝尔群而得到同样的结果. 霍夫曼 (Hoffman [1]) 假定 G 是循环作用在 π 的不属于 L_∞ 而且不是原点的 $n^2 - 1$ 个点上的群而得到类似的结果.

假定给了阶为 n 的平面 π 的直射群 G, 设 G 是阿贝尔群而且在 π 的 N 个点上是传递的和正则的. 这时如果 P 是 π 的一个不变点, 则 π 的每个点有唯一的表示 Px, $x \in G$. 如果整数 t 与 N 互素,则 $x \to x^t$ 对于全体 $x \in G$ 显然是 G 的自同构. 再有,如果对于每个 $x \in G$, $P_x \to Px^t$ 是 π 的直射, 则我们说 t 是 π 的乘子. 乘子显然组成取模 N 的乘法群.

定理 20.9.11. 如果阶为 n 的平面 π 有直射群 G, 它是阿

贝尔群而且在 π 的 N 个点上是传递的和正则的，则整除 n 的每个素数 p 都是 π 的乘子.

证明. 在定理的假设下，只有点的一个传递组，因而也只有线的一个传递组. 存在单独一个代表点 $P = P_1$ 和单独一条代表线 $L = L_1$，而且如果 $D_{11} = \{x_1, x_2, \cdots, x_{n+1}\}$, $x_i \in G$，则 Px_i, $i = 1, \cdots, n+1$ 是 L_1 的点. 于是

$$x_1u, \cdots, x_{n+1}u (u \in G)$$

是 G 的点. 这时我们有 $D' = \delta_{11}$, $D = \delta^*_{11}$.

$$\begin{aligned} D &= x_1 + \cdots + x_{n+1}, \\ D' &= x_1^{-1} + \cdots + x_{n+1}^{-1}. \end{aligned} \tag{20.9.33}$$

C_2 和 C_1 简化成单位矩阵. 关系式 (20.9.25) 的前两个有形状

$$DD' = D'D = n \cdot 1 + \gamma \tag{20.9.34}$$

(20.9.25) 中的后两个关系式不过是指出在 D 和 D' 中有 $n+1$ 个元素. 为了证明 $Px \to Px^p$ 是 π 的直射，我们必须证明 Px_1^p, Px_2^p, $\cdots$, Px_{n+1}^p 在一条线上. 为此我们需要证明，对于某个 $u \in G$[1]，

$$D^{(p)} = x_1^p + \cdots + x_{n+1}^p = (x_1 + \cdots + x_{n+1})u, \tag{20.9.34*}$$

因为任意的线 Lu 的点是 Px_1u, Px_2u, $\cdots$, $Px_{n+1}u$. 反之，如果 (20.9.34)* 成立，则 Px_1^p, $\cdots$, Px_{n+1}^p 是 Lu 的点，因而一般地 $P(x_1v)^p$, $\cdots$, $P(x_{n+1}v)^p$ 是 Luv^p 的点，因而 $Px \to Px^p$ 是直射而且 p 是乘子. 对于这个定理，我们取 G 在整数上的群环作为群环 G^*. $G^*(\bmod p)$ 是具有取模 p 而简化的系数的环 G^*. 我们有

$$\begin{aligned} D^{(p)} &= x_1^p + \cdots + x_{n+1}^p \\ &\equiv (x_1 + \cdots + x_{n+1})^p = D^p (\bmod p), \end{aligned} \tag{20.9.35}$$

1) 因为原书有两个 (20.9.34) 式，为了不改动以后各式的编号，我们把下面这第二个 (20.9.34) 式改成 (20.9.34)* 以示区别. ——译者

因为多元项的系数是 p 的倍数而且 G 是阿贝尔群. G 是阿贝尔群的假设在这里用到,又在肯定关系式 $(x_i v)^p = x_i^p v^p$ 时和肯定 $x \to x^p$ 是 G 的自同构时也用到. 我们注意到,由于 $p|n$ 和 $N = n^2 + n + 1$, 我们有 $(p, N) = 1$. 又因为 $p|n$, 我们从 (20.9.34) 得出

$$DD' \equiv \gamma(\mathrm{mod}\, p). \tag{20.9.36}$$

乘上 D^{p-1}, 我们有

$$D^p D' \equiv D^{p-1}\gamma \equiv (n+1)^{p-1}\gamma \equiv \gamma(\mathrm{mod}\, p). \tag{20.9.37}$$

因此,从 (20.9.35) 得出

$$D^{(p)} D' \equiv \gamma(\mathrm{mod}\, p). \tag{20.9.38}$$

由此我们可以写出

$$D^{(p)} D' = \gamma + pR, \tag{20.9.39}$$

这里（以下正是我们证明的要点）由于在 $D^{(p)}D'$ 内全体系数都是非负的, 在 R 中的群元素的系数也是非负的, 而且根据 (20.9.38),每一项 $a_i u_i$, $u_i \in G$ 有 $a_i \equiv 1(\mathrm{mod}\, p)$, $a_i \geqslant 0$. 因而 $a_i \geqslant 1$ 而且 $(a_i - 1)/p$ 是非负的整数,这就是 u_i 在 R 中的系数. 因为 $x \to x^{-1} (x \in G)$ 是 G 的自同构,所以对于 $h \in G^*$,决定了一个自同构 $h \to h'$, 而且在这个自同构下有 $D \to D'$. 应用到(20.9.39), 这导出

$$DD'^{(p)} = \gamma + pR'. \tag{20.9.40}$$

其次, $x \to x^p$ 是 G 的自同构而且决定 G^* 的自同构 $h \to h^{(p)}$. 应用到 (20.9.34), 这导出

$$D^{(p)} D'^{(p)} = n \cdot 1 + \gamma. \tag{20.9.41}$$

(20.9.34) 和 (20.9.41) 的左边的乘积等于 (20.9.39) 和 (20.9.40) 的左边的乘积. 因此,右边的乘积也相等,即我们有

$$(n \cdot 1 + \gamma)^2 = (\gamma + pR)(\gamma + pR'). \tag{20.9.42}$$

把由 $x \to 1 (x \in G)$ 决定的从 G^* 到整数的同态应用到 (20.9.39), 给出

$$(n+1)^2 = n^2 + n + 1 + pR(1), \qquad (20.9.43)$$
这里在同态下 $R \to R(1)$. 因而 $pR(1) = n$, 又 $pR'(1) = n$. 但是在 G^* 内 $pR\gamma = pR(1)\gamma = n\gamma$. 把这用到(20.9.42)内. 我们得出

$$n^2 \cdot 1 = (pR)(pR') \qquad (20.9.44)$$
但是因为 pR 和 pR' 有非负的系数,当在 pR 内有多于一个非零的项时这是不可能的. 因此 $pR = bu$ 对于某个整数 b 和 $u \in G$. 但是 $b = pR(1) = n$, 因而 $pR = nu$. 代入(20.9.39), 我们有

$$D^{(p)}D' = \gamma + nu. \qquad (20.9.45)$$
乘上 D, 再利用(20.9.34), 我们有

$$\begin{aligned} D^{(p)}D'D &= \gamma D + nDu, \\ D^{(p)}(n+\gamma) &= (n+1)\gamma + nDu, \qquad (20.9.46) \\ nD^{(p)} + (n+1)\gamma &= (n+1)\gamma + nDu, \end{aligned}$$
这给出

$$D^{(p)} = Du. \qquad (20.9.47)$$
而这正是我们所需要的关系(20.9.34)*, 因而定理证明了.

为了说明这个定理的力量, 考虑具有阶为 73 的(必定循环的)直射群的 8 阶平面. 点可以用取模 73 的剩余来表示, 乘子是 2, 而且如果 $a_1, \cdots, a_9$ 是一条线上的点, 则 $2a_1, \cdots, 2a_9$ 对于适当的 s 是某个次序的 $a_1 + s, \cdots, a_9 + s$. 于是点 $a_1 - s, \cdots, a_9 - s$ 在被乘子 2 不变的一条线上. 如果这些剩余中有一个是 1, 则乘子 2 给出一条线上的完全的点组 1, 2, 4, 8, 16, 32, 37, 55, 64 (mod 73). 被 2 不变的任何其它点组只与这个组相差一个常数因子, 因而给出同一个平面. 这平面是德沙格平面.

修格斯还证明了进一步的一个结果, 它是比定理 20.9.10 既特殊又精细的.

定理 20.9.12. 当 $n\equiv 2(\mathrm{mod}4)$, $n>2$ 时，阶为 n 的平面不会有对合.

证明. 假定 π 是阶为 n 的平面，这里 $n\equiv 2(\mathrm{mod}4)$, $n>2$，它具有一个对合 b. 那么根据定理 20.9.7，因为 n 是偶数而且不是平方数，所以 b 是合射. 设 M 是合射的轴而且 $C\in M$ 是合射的中心. 设 Q_i, $i=1,\cdots,n$ 是 M 上的其余的点，而且 K_i, $i=1,\cdots,n$ 是通过 C 的其余的线. 记 $n=2m$，这里 m 是奇数. π 上不通过 C 的 n^2 条线可以分成 $n^2/2=2m^2$ 类，每一类包含两条直线，当其中一条是线 L 时，另一条是 Lb. 在每一类里取一条线 L_i, $i=1,\cdots,2m^2$. 同理，在线 K_i 上不是 C 的 n 个点可以被 b 分成 $n/2=m$ 类. 在每一类里取一个点而且把它记做 P_{ij}, $j=1,\cdots,n/2=m$. 我们现在用下列规则定义关联数 a_{ij}^k:

$$\begin{aligned}&a_{ij}^k=+1 \text{ 如果 } P_{ij}\in L_k,\\&a_{ij}^k=-1 \text{ 如果 } P_{ij}b\in L_k,\\&a_{ij}^k=0 \text{ (其他情形)}.\end{aligned}\qquad(20.9.48)$$

引理 20.9.3. $\sum_k (a_{ij}^k)^2=n.$

引理 20.9.4. $\sum_k a_{ij}^k a_{st}^k=0$ 如果 $(i,j)\neq(s,t)$.

引理 20.9.3. 的证明. 因为点 P_{ij} 在或是 L_k 或是 L_kb 的 n 条线上，所以有引理 20.9.3.

引理 20.9.4 的证明. 如果 $i=s$, $j\neq t$，则由于点 P_{ij} 和 $P_{ij}b$ 全都在 K_i 上而不会有两个同在任何别的线上，因而和式是零. 如果 $i\neq s$，设 $P_{ij}P_{st}$ 是 L_qx, $L_{ij}P_{st}b$ 是 L_ry，这里 x 和 y 是 1 或 b. 这时 $r\neq q$，因为如果 $r=q$, $x=y$，则 $L_qx=L_ry$ 包含 P_{st} 和 $P_{st}b$，而它们是 K_s 上的不同的点，这是一个矛盾. 又如果 $r=q$, $x=yb$，则 $L_qx=L_ryb$ 包含不同的点

P_{ij} 和 $P_{ij}b$，它们同在 K_i 上，这又是一个矛盾. 因此 $r \neq q$. 于是

$$a_{ij}^q = a_{st}^q,\ a_{ij}^q a_{st}^q = +1,$$

而且 $$a_{ij}^r = -a_{st}^r,\ a_{ij}^r a_{st}^r = -1.$$

因而引理 20.9.4 的非零项可以分成对，使每一对的和是零. 因此引理 20.9.4 的和式是零.

从引理出发,关联数 a_{ij}^k 可以组成一个 $2m^2 \times 2m^2$ 矩阵:

$$A = (a_{ij}^k),\ 其中\ ij\ 表示行，k\ 表示列， \qquad (20.9.49)$$

根据引理, A 满足

$$AA^T = nI. \qquad (20.9.50)$$

我们用下列规则定义 b_{ik}:

$$b_{ik} = \sum_{j=1}^{m} a_{ij}^k,\ i = 1, \cdots, n;\ k = 1, \cdots, 2m^2. \qquad (20.9.51)$$

那么每个 b_{ik} 是 $+1$ 或 -1,因为每条线 L_k 与 K_i 恰好相交于一个点 P_{ij} 或 $P_{ij}b$, 所以恰好有一个 a_{ij}^k 不是零. 下列 $n \times 2m^2$ 矩阵 B 是这样的:

$$B = (b_{ik}),\ i = 1, \cdots, n;\ k = 1, \cdots, 2m^2, \qquad (20.9.52)$$

它的第一行是 A 的前 m 行之和，它的第二行是 A 的次 m 行之和,等等. 因为根据(20.9.50)，A 的不同的行的内积是零,所以对于 B 的行也有同样结果. 我们可以用 $+1$ 或 -1 乘 B 的列而不改变内积,而这样做可以使 B 的第一行只包含$+1$. 因为 $n > 2$, 所以 B 至少有三行，重新排列 B 的列，可以使 B 的前三行取下列形式:

$$\left|\begin{array}{cc|cc}
\multicolumn{2}{c|}{+1, \quad \cdots, \quad +1} & \multicolumn{2}{c}{+1, \quad \cdots, \quad +1} \\
\hline
+1,\cdots,+1 & +1,\cdots,+1 & -1,\cdots,-1 & -1,\cdots,-1 \\
+1,\cdots,+1 & -1,\cdots,-1 & +1,\cdots,-1 & -1,\cdots,-1
\end{array}\right|$$

$$r\ 列 \qquad s\ 列 \qquad t\ 列 \qquad u\ 列$$

$$(20.9.53)$$

因为第二和第三行与第一行的内积等于零，所以 $r+s=t+u$; $r+t=s+u$. 这时 $r+s+t+u=2m^2$, 因而:

$$r+s=t+u=m^2,\ r+t=s+u=m^2, \quad (20.9.54)$$

于是

$$u=r,\ s=t=m^2-r. \quad (20.9.55)$$

因为第二行和第三行的内积也是零，所以 $r+u=s+t=m^2$. 而这给出

$$2r=m^2 \quad (20.9.56)$$

由于 $n\equiv 2\ (\mathrm{mod} 4)$, $n=2m$ 而且 m 是奇数，上式是一个矛盾. 因此 π 不能有对合，而我们的定理也就证明了. 这个结果也可以从(20.9.25)的关联关系经过适当的重新编号并利用由同态 $1\to 1$, $b\to -1$ 决定的从 G^* 到整数上的映射而得到.

韦勃伦和魏德本 (Veblen and Wedderburn[1]) 给过阶为9的非德沙格平面的例子. 修格斯 (Hughes [2]) 证明这个例子是一个无限类的一个特殊情形. 设 $q=p^r$ 是奇素数 p 的方幂. 我们曾证明过，存在阶为 q^2 的准域 K, 它的中心 Z 是域 $GF(q)=GF(p^r)$. 修格斯平面的阶是 q^2.

修格斯平面的定义. 点 P 是三元组的集合 $P=(xk, yk, zk)$, x, y, z 是 K 的不全是零的固定元素而且 $k\neq 0$ 是 K 的任意元素. 辛格尔定理 20.9.5 给我们一个映射

$$\begin{aligned} x &\to a_{11}x+a_{12}y+a_{13}z,\\ y &\to a_{21}x+a_{22}y+a_{23}z,\\ z &\to a_{31}x+a_{32}y+a_{33}z, \end{aligned} \quad (20.9.57)$$

这里 $a_{ij}\in Z$, 使得

$$(x, y, z)=P\to PA=(a_{11}x\cdots, \cdots, \cdots a_{33}z) \quad (20.9.58)$$

是用 Z 建立坐标的 q 阶德沙格平面的阶为 $m=q^2+q+1$ 的直射 α. 修格斯平面是经过把直射 α 扩展到具有 K 中的坐

标的点而给出的.

我们有由方程

$$x + ty + z = 0 \qquad (20.9.59)$$

给出的基线. 这里我们取 $t = 1$ 或 $t \notin Z$, 而在其余的情形 t 是 K 的任意元素. 这给出 $1 + (q^2 - q) = q^2 - q + 1$ 条基线. 我们定义关联关系 $P = (xk, yk, zk) \in L_t$, 必要而且只要 x, y, z 满足 (20.9.59). 根据 K 中乘法的结合性和右分配律, 从 (20.9.59) 我们还有

$$0 = (x + ty + z)k = xk + t(yk) + zk. \qquad (20.9.60)$$

因而关联关系 $P \in L_t$ 不依赖于 P 的适合 (20.5.59) 的表示的选取. 然后用记号 $L_t\alpha^i$, $i = 0, \cdots, m - 1$ 表示其余的线, 而且认为

$$PA^i \in L_t\alpha^i, i = 0, \cdots, m - 1, \qquad (20.9.61)$$

必要而且只要 $P \in L_t$.

$L_t\alpha^i$ 的点并不一定满足一个线性方程. 为了找出 L_t 上的点, 我们可以在 (20.9.59) 中任意地取 x 和 y, 只要不同时取零, 然后从方程决定 z. 这样得出 $q^4 - 1$ 个三元组, 其中每 $q^2 - 1$ 个表出同一个点. 因此 L_t 包含 $q^2 + 1 = n + 1$ 个不同的点. 因此 $L_t\alpha^i$ 也包含 $n + 1$ 个点. 我们一共有

$$(q^2 - q + 1)(q^2 + q + 1) = q^4 + q^2 + 1 = n^2 + n + 1$$

条线, 每一条都包含 $n + 1$ 个点. 一共有 $n^2 + n + 1$ 个点. 因而为了证明这是一个射影平面, 只要证明任何两条不同的线有唯一的公共点. 映射 $P \to PA$ 是一一的而且有周期 $m = q^2 + q + 1$. 如果 $\{P\}_s$ 是基线 L_s 上的点集, 则 $L_s\alpha^i$ 的点集是 $\{P\}_sA^i$, 而且 $L_t\alpha^j$ 的点集是 $\{P\}_tA^j$. 因此为了证明 $L_s\alpha^i$ 和 $L_t\alpha^j$ 有唯一的公共点, 只要证明 L_s 和 $L_t\alpha^{j-i} = L_t\alpha^h$ (这里 α 的方次数是对模 m 取的) 有唯一的公共点.

设 $P = (x, y, z)$ 是 $L_t\alpha^h$ 的点. 那么 PA^{-h} 是 L_t 的点,

反之亦然．于是如果

$$(x, y, z)A^{-h} = (b_{11}x + b_{12}y + b_{13}z,$$
$$b_{21}x + b_{22}y + b_{23}z, b_{31}x + b_{32}y + b_{33}z), \quad (20.9.62)$$

则 $P = (x, y, z)$ 在 $L_t\alpha^h$ 上的条件是

$$(b_{11}x + b_{12}y + b_{13}z) + t(b_{21}x + b_{22}y + b_{23}z)$$
$$+ (b_{31}x + b_{32}y + b_{33}z) = 0 \quad (20.9.63)$$

如果 (x, y, z) 在 L_s 上，则我们有

$$x + sy + z = 0. \quad (20.9.64)$$

我们必须证明，不考虑在右边乘上一个因子 k，(20.9.63)和(20.9.64)有唯一的解 (x, y, z)．我们对 x 解出(20.9.64)而且代入(20.9.63)．这给出

$$uy + az + t(vy + bz) = 0, \quad (20.9.65)$$

这里

$$\begin{aligned} u &= b_{12} + b_{32} - (b_{11} + b_{31})s, \\ v &= b_{22} - b_{21}s, \\ a &= b_{13} + b_{33} - (b_{11} + b_{31}), \\ b &= b_{23} - b_{21}. \end{aligned} \quad (20.9.66)$$

注意 $a, b \in Z$，但是 u, v 一般不在 Z 内．在找(20.9.65)的解时需要考虑三种情形．

情形 1. $b \neq 0$，这时(20.9.65)可以写成

$$(b^{-1}a + t)(vy + bz) + (u - b^{-1}av)y = 0, \quad (20.9.67)$$

这里用到 a 和 b^{-1} 在中心内的事实．如果系数 $b^{-1}a + t$ 和 $u - b^{-1}av$ 都是零，则 $t \in Z$，$t = 1$，而且 $a + b = 0$，$u + v = 0$．但是这时从 $u + v = 0$ 得出

$$b_{12} + b_{22} + b_{32} = (b_{11} + b_{21} + b_{31})s, \quad (20.9.68)$$

因而 $s \in Z$，即 $s = 1$．于是 $a + b = 0$ 给出

$$b_{13} + b_{23} + b_{33} = b_{11} + b_{21} + b_{31}. \quad (20.9.69)$$

连同 $s=1$ 和 $t=1$，这说明(20.9.63)和(20.9.64)表出 $GF(q)$

上的德沙格平面 π_1 的同一条线. 而由于矩阵 A 作为 π_1 的直射是 $m = q^2 + q + 1$ 阶的，所以除非 $L_s = L_1$, $L_t\alpha^i = L_1$，上述结论不可能成立. 因此 (20.9.67) 中的系数不全是零. 因而如果 $b^{-1}a + t \neq 0$，则 y 的任意值唯一地决定 $vy + bz$，而且因为 $b \neq 0$，它唯一地决定 z. 如果 $b^{-1}a + t = 0$，则 $u - b^{-1}av \neq 0$ 因而 $y = 0$，于是 z 是任意的. 因此除去可以相差一个右因子，y 和 z 唯一地决定，然后从(20.9.64)，x 由 y 和 z 唯一决定. 因而(20.9.63)和(20.9.64)被唯一的点 (xk, yk, zk) 所满足. 这就在情形 1 下给出所要的唯一解.

情形 2. $b = 0$, $a \neq 0$，这时 (20.9.65) 变成

$$(u + tv)y + az = 0. \qquad (20.9.70)$$

因为 $a \neq 0$，(20.9.70) 和 (20.9.64) 被唯一的点 (xk, yk, zk) 所满足.

情形 3. $b = 0$, $a = 0$. 这时我们有

$$b_{13} + b_{33} = b_{11} + b_{31},$$
$$b_{23} = b_{21}, \qquad (20.9.71)$$

而且我们发现点 $P = (k, 0, -k)$ 同时满足 (20.9.65) 和 (20.9.64). 又根据 (20.9.71)，我们从 (20.9.62) 得出

$$PA^{-h} = (k, 0, -k)A^{-h}$$
$$= (b_{11} - b_{13})(k, 0, -k) = P, \qquad (20.9.72)$$

这里因为 A^{-k} 不是奇异的，$b_{11} - b_{13} \neq 0$. 于是因为 A^h 不变 π_1 的点 P，我们得出 $h \equiv 0 \pmod{m}$，因而 $L_t\alpha^h$ 是 L_t. 因此我们的线现在是 L_s 和 L_t，这里当然有 $s \neq t$. 对于这两条线，$x + sy + z = 0$ 和 $x + ty + z = 0$，因而显然有 $P = (k, 0, -k)$ 同时在这两条线上而没有其它的点是如此的. 总之在每一种情形里，任何两条不同的线有唯一的交点，因而我们证明了它们组成射影平面. 我们把这写成一个定理.

定理 20.9.13 (修格斯). 给了阶为 q^2 的准域 K，它的中

心是 $GF(q)=Z$，$q=p^r$，p 是奇素数，而且由(20.9.57)决定的阶为 q^2+q+1 的映射 A 是阶为 q 的德沙格平面的直射．那么按照规则(20.9.59)和(20.9.61)而包含点 PA^i 的线 $L_t\alpha^i$ 组成阶为 q^2 的射影平面 π.

修格斯还证明，如果准域 K 不是域 $GF(q^2)$，则平面 π 不仅是非德沙格的，而且不是在任何坐标系里的韦勃伦-魏德本平面.

参 考 文 献

Albert, A. A.

[1] On nonassociative division algebras, *Trans. Amer. Math. Soc.*, **72**(1952). 296—309.

Baer, R.

[1] Erweiterung von Gruppen und ihrer Isomorphismen, *Math. Zeit.*, **38**(1934), 375—416.

[2] The decomposition of enumerable primary Abelian groups into direct summands, *Quart. J. of Math.*, **6**(1935), 217—221.

[3] The decomposition of Abelian groups into direct summands, *Quart. J. of Math.*, **6**(1935), 222—232.

[4] Types of elements and the characteristic subgroups of Abelian groups, *Proc. London Math. Soc.*, **39**(1935), 481—514.

[5] The subgroup of elements of finite order of an Abelian group, *Ann. of Math.*, **37**(1936), 766—781.

[6] Dualism in Abelian groups, *Bull. Amer. Math. Soc.*, **43**(1937), 121—124.

[7] Duality and commutativity of groups, *Duke Math. J.*, **5**(1939), 824—838.

[8] The significance of the system of subgroups for the structure of a group, *Amer. J. of Math.*, **61**(1939), 1—44.

[9] Abelian groups that are direct summands of every containing Abelian group, *Bull. Amer. Math. Soc.*, **46**(1940), 800—806.

[10] Homogeneity of projective planes, *Amer. J. of Math.*, **64**(1942), 137—152.

[11] Klassification der Gruppenerweiterungen, *J. reine angew. Math.*, **187**(1949), 75—94.

[12] Supersoluble groups, *Proc. Amer. Math. Soc.*, **6**(1955), 16—32.

Bethe, H. A.

[1] Termaufspaltung in Kristallen, *Ann. der Physik*, (5) **3**(1929), 133—208.

Birkhoff, Garrett

[1] Lattice Theory, Colloquium publications, Amer. Math. Soc., vol. XXV, rev ed., 1948.

Birkhoff, G., and MacLane, S.

[1] A Survey of Modern Algebra, The Macmillan Co., revised edi-

tion, 1953.

Bruck, R. H.

[1] Difference sets in a finite group, *Trans. Amer. Math. Soc.*, 78 (1955), 464—481.

Bruck, R. H., and Kleinfeld, E.

[1] The structure of alternative division rings, *Proc. Amer. Math. Soc.*, **2**(1951), 878—890.

Bruck, R. H., and Ryser, H. J.

[1] The non-existence of certain finite projective planes, *Can. J. Math.*, **1**(1949), 88—93.

Burnside, W.

[1] On an unsettled question in the theory of discontinuous groups. *Quart. J. Pure and Appl. Math.*, **33**(1902), 230—238.

[2] Theory of Groups of Finite Order, Cambridge Univ. Press, 2nd ed., 1911.

Chowla, S., and Ryser, H. J.

[1] Combinatorial problems, *Can. J. Math.*, **2**(1950), 93—99.

Eckmann, B.

[1] Cohomology of groups and transfer, *Ann. of Math.*, **58**(1953), 481—493.

Eilenberg, S., and MacLane, S.

[1] Cohomology theory in abstract groups I, *Ann. of Math.*, 48 (1947), 51—78.

[2] Cohomology theory in abstract groups II, *Ann. of Math.*, 48 (1947), 326—41.

Federer, H., and Jonsson, B.

[1] Some properties of free groups, *Trans. Amer. Math. Soc.*, 68 (1950), 1—27.

Frobenius, G.

[1] Über auflösbare Gruppen IV, *Berl. Sitz.*, **1901**, 1223—1225.

[2] Über einen Fundamentalsatz der Gruppentheorie, *Berl. Sitz.*, **1903**, 987—991.

Gaschütz, W.

[1] Zur Erweiterungstheorie der Endlichen Gruppen, *J. reine angew. Math.*, **190**(1952); 93—107.

Gleason, A. M.

[1] Finite Fanao planes, *Amer. J. Math.*, 78(1956), 797—807.

Grün, O.

[1] Beiträge zur Gruppentheorie I, *J. reine angew. Math.*, **174**(1935), 1—14.

Hall, Marshall, Jr.

[1] Group rings and extensions, *Ann. of Math.*, **39**(1938), 220—234.
[2] Projective planes, *Trans. Amer. Math. Soc.*, **54**(1943), 229—277; Correction, *Trans. Amer. Math. Soc.*, **65**(1949), 473—474.
[3] Cyclic projective planes, *Duke Math. J.*, **14**(1947), 1079—1090.
[4] Coset representation in free groups, *Trans. Amer. Math. Soc.*, **67**(1949), 421—432.
[5] Subgroups of finite index in free groups, *Can. J. Math.*, **1**(1949), 187—190.
[6] A basis for free Lie rings and higher commutators in free groups, *Proc. Amer. Math. Soc.*, **1**(1950), 575—581.
[7] Subgroups of free products, *Pacific J. Math.*, **3**(1953), 115—120.
[8] On a theorem of Jordan, *Pacific J. Math.*, **4**(1954), 219—226.
[9] Solution of the Burnside problem for exponent 6, *Proc. Nat. Acad. Sci.*, **43**(1957), 751—753.

Hall, M. Jr., and Rado, T.
[1] On Schreier systems in free groups, *Trans. Amer. Math. Soc.*, **64**(1948), 386—408.

Hall, M. Jr., and Ryser, H. J.
[1] Normal completions of incidence matrices, *Amer. J. Math.*, **76** (1954), 581—589.

Hall, Philip
[1] A note on soluble groups, *J. London Math. Soc.*, **3**(1928), 98—105.
[2] A contribution to the theory of groups of prime-power order, *Proc. London Math. Soc.*, **36**(1933), 29—95.
[3] On a Theorem of Frobenius, *Proc. London Math. Soc.*, **40**(1936), 468—501.

Hall, P., and Higman, G.
[1] The p-length of a p-soluble group, and reduction theorems for Burnside's problem, *Proc. London Math. Soc.*, (3) **7**(1956), 1—42.

Hardy, G. H., and Wright, E. M.
[1] An Introduction to the Theory of Numbers, The Clarendon Press, Oxford, 1938.

Higman, Graham
[1] On finite groups of exponent five, *Proc. Camb. Phil. Soc.*, **52** (1956), 381—390.

Hirsch, K. A.
[1] On infinite soluble groups, *Proc. London Math. Soc.*, (2) **44** (1938), 53—60.

[2] On infinite soluble groups II, *Ibid.*, **44**(1938), 336—344.
[3] On infinite soluble groups III, *Ibid.*, **49**(1946), 184—194.

Hoffman, A. J.

[1] Cyclic affine planes, *Can. J. Math.*, **4**(1952), 295—301.

Hölder, O.

[1] Zuruckführung einer beliebigen algebraischen Gleichung auf eine Kette von Gleichungen, *Math. Ann.*, **34**(1889), 26—56.

Holyoke, T. C.

[1] On the structure of multiply transitive permutation groups, *Amer. J. Math.*, **74**(1952), 787—796.

Hughes, D. R.

[1] Regular collineation groups, *Proc. Amer. Math. Soc.*, **8**(1957), 159—164.
[2] A class of non-Desarguesian projective planes, *Can. J. Math.*, **9**(1957), 378—388.
[3] Generalized incidence matrices over group algebras, Ill. *J. Math.*, **1**(1957), 545—551.
[4] Collineations and generalized incidence matrices, *Trans. Amer. Math. Soc.*, **86**(1957), 284—296.

Huppert, B.

[1] Normalteiler und maximale Untergruppen endlicher Gruppen, *Math. Zeit.*, **60**(1954), 409—434.

Iwasawa, K.

[1] Über die endlichen Gruppen und die Verbände ihrer Untergruppen, *J. Univ. Tokyo.*, **43**(1941), 171—199.

Jordan, C.

[1] Commentaire sur Galois, *Math. Ann.*, **1**(1869), 141—160.
[2] Recherches sur les substitutions, *J. Math. Pures Appl.*, (2) **17** (1872), 351—363.

Kaplansky, I.

[1] Infinite Abelian Groups, University of Michigan Press, 1954.

Kleinfeld, E.

[1] Alternative division rings of characteristic 2, *Proc. Nat. Acad. Sci. USA.*, **37**(1951), 818—820.
[2] Right alternative rings, *Proc. Amer. Math. Soc.*, **4**(1953), 939—944.

Kostrikin, A. I.

[1] Solution of the restricted Burnside problem for exponent 5, *Izv. Akad. Nauk SSSR, Ser mat.*, **19**(1955), 233—244. (In Russian.)

Krull, W.

[1] Über verallgemeinerte endliche Abelsche Gruppen, *Math. Zeit.*, **23**(1925), 161—196.

[2] Theorie und Anwendung der verallgemeinerten Abelschen Gruppen, *Sitz Heidelberg. Akad. Wiss.*, **1926**, 1—32.

Kurosch, A.

[1] Die Untergruppen der freien Produkte von beliebigen Gruppen, *Math. Ann.*, **109**(1934), 647—660.

[2] The Theory of Groups, 2nd. ed., translated from the Russian by K. A. Hirsch, two volumes, Chelsea Publishing Co., New York, 1955. (中译本：A. 库罗什，群论，人民教育出版社，1964.)

Levi, F. W.

[1] Über die Untergruppen der freien Gruppen, *Math. Zeit.*, **32**(1930), 315—318.

Levi, F. W., and van der Waerden, B. L.

[1] Über eine besondere Klasse von Gruppen, *Abh. Math. Sem. Hamburg*, **9**(1933), 154—158.

MacLane, S.

[1] A conjecture of Ore on chains in partially ordered sets, *Bull. Amer. Math. Soc.*, **49**(1943), 567—568.

[2] Cohomology theory in abstract groups, III, *Ann. of Math.*, **50** (1949), 736—761.

Magnus, W.

[1] Über Bezhieungen zwischen höheren Kommutatoren, *J. reine angew. Math.*, **177**(1937), 105—115.

[2] On a theorem of Marshall Hall, *Ann. of Math.*, **40**(1939). 764—768.

[3] A connection between the Baker-Hausdorff formula and a problem of Burnside, *Ann. of Math.*, **52**(1950), 111—126.

Mann, H. B.

[1] On certain systems which are almost groups, *Bull. Amer. Math. Soc.*, **50**(1944), 879—881.

Meier-Wunderli, H.

[1] Note on a basis for higher commutators, *Commentarii Math. Helvetici*, **16**(1951), 1—5.

Miller, G. A.

[1] Limits of the degree of transitivity of substitution groups, *Bull. Amer. Math. Soc.*, **22**(1915), 68—71.

Moufang, R.

[1] Alternativkörper und der Satz vom vollständigen Vierseit, *Abh. Math. Sem. Hamburg*, **9**(1933), 207—222.

Neumann, B. H.

[1] Die Automorphismengruppe der freien Gruppen. *Math. Ann.*, **107**(1932), 367—386.

[2] On the number of generators of a free product, *J. London Math. Soc.*, **18**(1943), 12—20.

Neumann, H.

[1] Generalized free products with amalgamated subgroups I, *Amer. J. Math.*, **70**(1948), 590—625.

[2] Generalized free products with amalgamated subgroups II, *Ibid.*, **71**(1949), 491—540.

Nielsen, J.

[1] Om Regnig med ikke-kommutative Faktorer og dens Anvendelse i Gruppeteorien, *Mat. Tidsskrift* B, **1921**, 77—94.

Noether, E.

[1] Hyperkomplexe Zahlen und Darstellungstheorie, *Math. Zeit.*, **30** (1929), 641—692.

Ore, O.

[1] Direct Decompositions, *Duke Math. J.*, **2**(1936), 581—596.

[2] On the theorem of Jordan-Hölder, *Trans. Amer. Math. Soc.*, **41** (1937), 266—275.

[3] Chains in partially ordered sets, *Bull. Amer. Math. Soc.*, **49** (1943), 558—566.

Ostrom, T. G.

[1] Double transitivity in finite projective planes, *Can. J. Math.*, **8** (1956), 563—567.

Parker, E. T.

[1] On collineations of symmetric designs, *Proc. Amer. Math. Soc.*, **8**(1957), 350—351.

Pauli, W.

[1] Zur Quantenmechanik des Magnetischen Elektrons, *Zeit. für Physik*, **43**(1927), 601—623.

Pickert, G.

[1] Projektive Ebenen, Springer (1955).

Pontrjagin, L.

[1] Topological Groups, translated from the Russian by Emma Lehmer, Princeton University Press, 1939.(中译本: L. 邦德列雅金,连续群,科学出版社,上册,1957; 下册,1958.)

Prüfer, H.

[1] Theorie der abelschen Gruppen I, *Math. Zeit.*, **20**(1924), 165—187.

[2] Theorie der abelschen Gruppen II, *Math. Zeit.*, **22**(1925), 222—249.

Remak, R.

[1] Über die Zerlegung der endlichen Gruppen in direkte unzerlegbare Faktoren, *J. reine angew. Math.*, **139**(1911), 293—308.

[2] Über die Zerlegung der endlichen Gruppen in direkte unzerlegbare Faktoren, *J. reine angew. Math.*, **153**(1923), 131—140.

Sanov, I. N.

[1] Solution of Burnside's problem for exponent 4, *Leningrad State Univ. Ann.*, **10**(1940), 166—170. (In Russian.)

San Soucie, R. L.

[1] Right alternative division rings of characteristic two, *Proc. Amer. Math. Soc.*, **6**(1955), 291—296.

Schmidt, O.

[1] Über die Zerlegung endlicher Gruppen in direkte unzerlegbare Faktoren, *Izvestiya Kiev Univ.*, **1912**, 1—6.

Schreier, O.

[1] Über die Erweiterung von Gruppen, I, *Monats. für Math. u. Phys.*, **34**(1926), 165—180.

[2] Über die Erweiterung von Gruppen II, *Abh. Math. Sem. Hamburg*, **4**(1926), 321—346.

[3] Die Untergruppen der freien Gruppen, *Abh. Math. Sem. Hamburg*, **5**(1927), 161—183.

[4] Über den Jordan-Hölderschen Satz, *Abh. Math. Sem. Hamburg*, **6**(1928), 300—302.

Singer, J.

[1] A theorem in finite projective geometry and some applications to number theory, *Trans. Amer. Math. Soc.*, **43**(1938), 377—385.

Skornyakov, L. A.

[1] Alternative fields, *Ukrain. Mat. Zur.*, **2**(1950), 70—85. (In Russian.)

[2] Right alternative fields, *Izv. Akad. Nauk SSSR, Ser. Mat.*, **15** (1951), 177—184. (In Russian.)

Suzuki, M.

[1] Structure of a group and the structure of its lattice of subgroups, Ergebnisse der Mathematik und ihrer Grenzgebiete, **10**(1956), Springer, Berlin.

Tarry, G.

[1] Le problème des 36 officiers, *C. R. Assoc. Fr. Av. Sci.*, **1900**, 122—123; and (1901), 170—203.

Ulm, H.

[1] Zur Theorie der abzählbar unendlichen abelschen Gruppen, *Math.*

Ann., **107**(1933), 774—803.

van der Waerden, B. L.

[1] Moderne Algebra, 2nd ed., Berlin, 1940.(中译本: B.L.范·德·瓦尔登,代数学,科学出版社, (I), 1963; (II), 1976.)

Veblen, O., and Wedderburn, J. H. M.

[1] Non-Desarguesian and non-Pascalian geometries, *Trans. Amer. Math. Soc.*, **8**(1907), 379—388.

Veblen, O., and Young, J, W.

[1] Projective Geometry, vol. 1, Ginn and Co., 1910.

Wedderburn, J. H. M.

[1] On the direct product in the theory of finite groups, *Ann. of Math.*, **10**(1909), 173—176.

Wielandt, H.

[1] Abschatzungen für den Grad einer Permutationsgruppe von vorgeschriebenem Transitivitätsgrad, *Schriften des Math. Sem. und des Inst. für angew. Math. der Univ. Berlin*, **2**(1934), 151—174.

[2] Eine Verallgemeinerung der invarianten Untergruppen, *Math. Zeit.*, **45**(1939), 209—244.

[3] p-Sylowgruppen und p-Faktorgruppen, *J. reine angew. Math.*, **182**(1940), 180—193.

Witt, E.

[1] Über die Kommutativität endlicher Schiefkörper, *Abh. Math. Sem. Hamburg*, **8**(1931), 413.

[2] Treue Darstellung Liescher Ringe, *J. reine angew. Math.*, **177**(1937), 152—160.

Zassenhaus, H.

[1] Zum Satz von Jordan-Hölder-Schreier, *Abh. Math. Sem. Hamburg*, **10**(1934), 106—108.

[2] Über endliche Fastkörper, *Abh. Math. Sem. Hamburg*, **11**(1936), 187—220.

Zorn, M.

[1] Theorie der alternativen Ringe, *Abh. Math. Sem. Hamburg*, **8**(1931), 123—147.

索　引

一　画

二　画

三　画

四　画

五　画

六　画

七 画

八 画

九 画

十 画

十一画

十二画

十 三 画

十 四 画

十 五 画

十六画以上

人 名 索 引

三 画

四 画

五 画

六 画

七 画

八 画

九 画

十 画

十 一 画

十 二 画

十 三 画

十 四 画

十五画以上

特殊记号索引

本书采用的一系列记号是标准的，其中包括：集合包含式记号 $A \supseteq B$ 是说 A 包含 B，$A \supset B$ 是说 A 真包含 B，$A \subseteq B$ 是说 A 包含在 B 内，$A \subset B$ 是说 A 真包含在 B 内；$a \in A$ 是说 a 属于集合 A；$a|b$ 是说 a 整除 b，$a \equiv b\ (\mathrm{mod}\, m)$ 是说 a 取模 m 而与 b 同余．还有下列标准用法，在记号上加一短线来表示关系的否定，例如：$p \nmid s$ 是说 p 不整除 s，$y \notin G$ 是说 y 不属于 G.

[General Information]
书名=群论
作者=（美）M·赫尔
页数=500
SS号=10068998
出版日期=1981年03月第1版